

**INSTITUTO DE ESTUDOS SUPERIORES MILITARES**  
**CURSO DE PROMOÇÃO A OFICIAL GENERAL**

**ANO LECTIVO 2005/ 2006**

**TRABALHO INDIVIDUAL DE LONGA DURAÇÃO**

***AS NOVAS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO***  
***E***  
***O NÍVEL OPERACIONAL DA GUERRA***

*Impacto no Planeamento e Condução das Operações Militares*

**RUI MANUEL DA SILVA RODRIGUES**  
***Coronel de Transmissões (Eng.)***

**ESTE TRABALHO É PROPRIEDADE DO INSTITUTO DE ESTUDOS  
SUPERIORES MILITARES**

**ESTE TRABALHO FOI ELABORADO COM FINALIDADE  
ESSENCIALMENTE ESCOLAR, DURANTE A FREQUÊNCIA DE UM  
CURSO DO INSTITUTO DE ESTUDOS SUPERIORES MILITARES,  
CUMULATIVAMENTE COM A ACTIVIDADE ESCOLAR NORMAL. AS  
OPINIÕES DO AUTOR, EXPRESSAS COM TOTAL LIBERDADE  
ACADÉMICA, REPORTANDO-SE AO PERÍODO EM QUE FORAM  
ESCRITAS, PODEM NÃO REPRESENTAR DOCTRINA SUSTENTADA  
PELO INSTITUTO DE ESTUDOS SUPERIORES MILITARES.**



## Abstract

*The future is not what it used to be*  
Anonymous

All along Alvin Toffler's first to the third civilisational wave, warfare has suffered major changes and "improvements". State of the art Communications and Information Technologies have induced a Revolution in Military Affairs, pushing warfare into the Information Age. Concepts like Network Centric Warfare (NCW) and Network Enabled Capability (NEC) became the new tenets of the evolution in warfare business.

Portugal, as a founding member of the Alliance could not help being dragged into this adventure. The technology evolution and the modern ways of warfare, asymmetric ones, shattered the traditional differences between levels of warfare, pushing the threshold of the operational down to what used to be the tactical level.

However, in a world where fighters overcame technological barriers through the adoption of asymmetric methodologies, technological superiority, although as far-fetched as it may be, no more equals to victory. Not disdaining technological advantages, especially the ones deriving from the "net centrality" concept, one must consider a deep change in leadership models in order to maximize the potential of the "network centric warfare".

Having that in mind, the the present work proposes to briefly analyse the impact of Communication and Information Systems Technologies at the planning and conduction of military operations, and more particularly the way the Portuguese Army is implementing Communication and Information Systems, within a future networked capability framework.

**Key words:** Information and Communications Technology, Information Systems, Command and Control, Network Centric Warfare, Leadership

## Resumo Analítico

*The future is not what it used to be*  
Anonymous

A guerra tem vindo a sofrer alterações e ”melhoramentos” em paralelo com a evolução civilizacional, desde a 1ª até à 3ª vaga de Alvin Toffler. As Tecnologias de Informação e Comunicação do “estado da arte” empurraram definitivamente a guerra para a Era da Informação. Termos como Network Centric Warfare (NCW) e Network Enabled Capability (NEC) transformaram-se nos novos conceitos que balizam a evolução na arte da guerra.

Portugal, enquanto membro fundador da Aliança, não pode ficar indiferente a esta aventura, em que a evolução tecnológica e as novas formas de conduzir a guerra, assimétricas, estilhaçam fronteiras entre os níveis da guerra, empurrando o nível operacional da guerra para o que costumava ser o nível tático.

Num mundo em que os beligerantes ultrapassam as disparidades tecnológicas usando meios assimétricos, a superioridade tecnológica, por muito pronunciada que seja, deixa de ser garante da supremacia. Sem menosprezar as vantagens que a tecnologia pode proporcionar, há que ponderar a introdução de alterações nos modelos de liderança para se conseguir maximizar as potencialidades desvendadas pelo conceito de “guerra centrada em rede”.

Neste enquadramento, o presente trabalho propõe-se analisar o impacto das tecnologias de Informação e Comunicação no planeamento e condução das operações militares e, mais particularmente, no modo como o Exército Português está a implementar os sistemas de informação e comunicações, numa perspectiva de capacidade centrada em rede.

**Palavras Chave :** Tecnologias de Informação e Comunicações, Sistemas de Informação, Comando e Controlo, Guerra Centrada em rede, Liderança.

## **LISTA DE ACRÓNIMOS**

<b>AC</b>	Active Component
<b>ACT</b>	Allied Command Transformation
<b>ADM</b>	Armas de Destruição Maciça
<b>AM</b>	Academia Militar
<b>BICES</b>	Battlefield Information and Communications Exploitation System
<b>BLOS</b>	Beyond Line of Sight
<b>BOA</b>	Bulle Opérationelle Aero terrestre
<b>C2</b>	Command and Control
<b>C2PC</b>	Command and Control Personal Computer, (Information System)
<b>C3</b>	Command, Control and Communications (ou Consultation)
<b>C4I</b>	Comando, Controlo, Comunicações, Computadores e Informações
<b>C4ISR</b>	Command, Control, Communications (ou Consultation), Computers, Intelligence, Surveillance and Reconnaissance
<b>CAOC</b>	Combined Air Operations Centre
<b>CAX</b>	Computer Aided Exercises
<b>CCEM</b>	Conselho de Chefes de Estado Maior
<b>CEDN</b>	Conceito Estratégico de Defesa Nacional
<b>CEM</b>	Conceito Estratégico Militar
<b>CEME</b>	Chefe do Estado Maior do Exército
<b>CEMGFA</b>	Chefe do Estado Maior General das Forças Armadas
<b>CIE</b>	Centro de Informática do Exército
<b>CIS</b>	Communications and Information Systems
<b>CNR</b>	Combat Net Radio
<b>COFT</b>	Comando Operacional das Forças Terrestres
<b>COP</b>	Common Operational Picture
<b>COTS</b>	Commercial Off The Shelf
<b>CSDN</b>	Conselho Superior de Defesa Nacional

<b>CSM</b>	Conselho Superior Militar
<b>CWID</b>	Coalition Warrior Interoperability Demonstration
<b>DoD</b>	Department of Defense
<b>DPP</b>	Divisão de Planeamento e Programação
<b>DST</b>	Direcção dos Serviços de Transmissões
<b>EAC</b>	Echelon Above Corps
<b>EBE</b>	Estrutura Base do Exército
<b>EMEL</b>	Escola Militar de Electromecânica
<b>EMGFA</b>	Estado Maior General das Forças Armadas
<b>EPT</b>	Escola Prática de Transmissões
<b>EUA</b>	Estados Unidos da América
<b>FA</b>	Forças Armadas
<b>FASS</b>	Functional Area Sub-System
<b>FBCB2</b>	Force XXI Battle Command Brigade and Below
<b>FCS</b>	Future Combat System
<b>FND</b>	Forças Nacionais Destacadas
<b>FOPE</b>	Força Operacional Permanente do Exército
<b>GIG</b>	Global Information Grid
<b>GPS</b>	Global Positioning System
<b>HLA</b>	High Level Architecture
<b>ICC</b>	Integrated Air Command and Control for Air Operations, ex-Interim CAOC's Capability
<b>IEG</b>	Information Exchange Gateway
<b>IESFA</b>	Infra Estrutura Segura das Forças Armadas ex-RESFA ( Rede Segura das Forças Armadas)
<b>IESM</b>	Instituto de Estudos Superiores Militares
<b>IFFN</b>	Identification Friend, Foe or Neutral (Identificação Amigo-Inimigo ou Neutro)
<b>IPLD</b>	Individual Position Locator Device

<b>ISDN</b>	Integrated Services Digital Network
<b>ISR</b>	Intelligence, Surveillance and Reconnaissance
<b>ISTAR</b>	Intelligence, Surveillance, Target Acquisition and Reconnaissance
<b>IVR</b>	Informações, Vigilância e Reconhecimento
<b>I&amp;D</b>	Investigação e Desenvolvimento
<b>JOIS</b>	Joint OPS/INTEL Information System
<b>JOpsC</b>	Joint Operations Concept
<b>JTRS</b>	Joint Tactical Radio System
<b>LAS</b>	Local Area System
<b>LCC</b>	Land Component Command
<b>LOBOFA</b>	Lei Orgânica de Bases da Organização das Forças Armadas
<b>LOCE</b>	Linked Operational Intelligence Centres Europe.
<b>LPM</b>	Lei de Programação Militar
<b>MAF</b>	Missão de Acompanhamento e Fiscalização
<b>MCCIS</b>	Maritime Command and Control Information System
<b>MDN</b>	Ministro da Defesa Nacional
<b>MIFA</b>	Missões das Forças Armadas
<b>NATO</b>	North Atlantic Treaty Organization
<b>NC3A</b>	NATO C3 Agency
<b>NC3B</b>	NATO C3 Board
<b>NCW</b>	Network Centric Warfare
<b>NEC</b>	Network Enabled Capability
<b>NGO</b>	Non Governmental Agency
<b>NNEC</b>	NATO Network Enabled Capability
<b>NRF</b>	NATO Response Force
<b>OD</b>	Organization Development
<b>OIF</b>	Operation Iraqi Freedom
<b>OOTW</b>	Operations Other Than War

<b>ONU</b>	Organização das Nações Unidas
<b>OTAN</b>	Organização do Tratado do Atlântico Norte
<b>PCC</b>	Prague Capabilities Commitment
<b>PMLP</b>	Plano de Médio e Longo Prazo
<b>RAP</b>	Radio Acces Point
<b>RMA</b>	Revolution in Military Affairs
<b>RSTA</b>	Reconnaissance, Surveillance and Target Acquisition
<b>RT</b>	Regimento de Transmissões
<b>SA</b>	Situation Awareness
<b>SAE</b>	Subsistema de Área Estendida
<b>SAL</b>	Subsistema de Área Local
<b>SATCOM</b>	SATellite COMunications
<b>SBCT</b>	Stryker Brigade Combat Team
<b>SCI2</b>	Sistema de Combate Integrado Individual
<b>SCRA</b>	Single Channel Radio Access
<b>SFN</b>	Sistema de Forças Nacional
<b>SHAPE</b>	Supreme Headquarters Allied Powers in Europe
<b>SICCE</b>	Sistema de Informação de Comando e Controlo do Exército
<b>SICOM</b>	Sistema Integrado de Comunicações Militares
<b>SICOMAR</b>	Sistema de Comunicações da Marinha
<b>SMCS</b>	System Management and Control Subsystem
<b>SIMOPMIL</b>	SIMulação de OPerações MILitares
<b>SIC-T</b>	Sistema de Informação e Comunicações Tático
<b>SIPRNET</b>	Secret Internet Protocol Router NET
<b>SITACO</b>	Sistema Tático de Comunicações
<b>SITEP</b>	Sistema de Telecomunicações do Exército Português
<b>SUM</b>	Sistema de Utilizadores Móveis

<b>TIC</b>	Tecnologias de Informação e Comunicações
<b>TIDE</b>	Transforming technology towards Information superiority, Decision superiority and Execution superiority
<b>UA</b>	Unit of Action
<b>UACV</b>	SIMulação de OPerações MILitares
<b>UAV</b>	Unmanned Aerial Vehicle
<b>UE<sub>x</sub></b>	Unit of Employment X
<b>UE<sub>y</sub></b>	Unit of Employment Y
<b>WAN</b>	Wide Area Network
<b>WAS</b>	Wide Area System

## ÍNDICE

<b>Capítulo 1 – INTRODUÇÃO</b>	<b>1</b>
<b>Capítulo 2 - O NÍVEL OPERACIONAL DA GUERRA</b>	<b>3</b>
2.1 Nível Operacional da Guerra. A Génese do conceito	3
2.2 Nível Operacional versus Arte Operacional	5
2.3 O Conflito ao Nível Operacional. Guerra de Informação	6
2.4 Evolução Futura	7
<b>Cap 3 - AS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÕES</b>	<b>9</b>
3.1 Os Sistemas de Informação	9
3.2 A Evolução dos Sistemas de Informação	10
3.3 As Revoluções nos Assuntos Militares	13
3.4 A Implementação das RAM. O Modelo YETTON	14
3.5 O Campo de Batalha do Sec XXI	14
<b>Capítulo 4 - IMPACTO DAS TIC NAS OPERAÇÕES</b>	<b>16</b>
4.1 Sistemas de Comando e Controlo e o Processo de Decisão Militar	16
4.2 Os novos Paradigmas da Guerra	16
4.3 A Transformação das Forças Terrestres. Implicações nos domínios da guerra	20
4.4 O Modelo Americano	26
4.5 O Modelo NATO	27
<b>Capítulo 5 - AS TIC NO EXÉRCITO PORTUGUÊS</b>	<b>29</b>
5.1 Enquadramento e Orientação Política	29
5.2 Planeamento de Médio e Longo Prazo. Plano Director de Sistemas de Informação	29
5.3 Sistema C4I	30
5.4 Info-estrutura do Exército	31
5.5 O Modo Conjunto	33
5.6 Simulação	34
5.7 Interoperabilidade	35
5.8 Indústria Nacional	36
5.9 Organização	36
5.10 Mudança de Mentalidades	38
<b>Capítulo 6 – CONCLUSÕES</b>	<b>39</b>
<b>BIBLIOGRAFIA</b>	
<b>Apêndices</b>	
<b>A : Glossário de Conceitos</b>	
<b>B : Ilustrações</b>	
<b>C : O Caso Português</b>	
<b>Anexos</b>	
<b>A : Evolução das Tecnologias de Informação e Comunicações</b>	
<b>B : Revoluções nos Assuntos Militares</b>	
<b>C : Exemplos</b>	
<b>D : Future Combat Systems</b>	
<b>E : Sistema de Informação e Comunicações Tático (SIC-T)</b>	



## Capítulo 1 – INTRODUÇÃO

*Nothing helps a fighting force more than correct information. Moreover, it should be in perfect order, and done well by capable personnel.*  
Che Guevara

Como consequência da revolução verificada na área das Tecnologias de Informação e de Comunicações (TIC), no dealbar da última década surgiram novas teorias, baseadas nos conceitos americanos de guerra centrada em rede (NCW) e do britânico NEC (Network Enabled Capability), este último também adoptado pela NATO como NATO Network Enabled Capability (NNEC), que se materializaram nas operações centradas em rede.

Numa era de soberania limitada, os Estados para se fazerem ouvir no areópago das nações têm de estar aptos a emparceirar, de pleno direito, com os aliados na defesa de causas comuns.

Estando os nossos parceiros na NATO a enveredar assumidamente por uma via de aplicação intensiva das Tecnologias de Informação e Comunicação (TIC) às operações militares e a reorganizar-se em torno dos novos conceitos daí decorrentes, Portugal, país periférico, que nunca conseguiu subtrair-se às grandes tendências da massa em que se insere, não pode deixar de seguir esta orientação.

O tema proposto, *As novas Tecnologias de Informação e Comunicação e o Nível Operacional da Guerra, Impacto no Planeamento e Condução das Operações Militares*, surge assim como um assunto de pleno interesse e actualidade, considerando a aposta do Exército Português nas novas tecnologias, consubstanciada nos produtos VIGRESTE e SICCE.

Como hipóteses, considerou-se que :

- a evolução das novas tecnologias de informação e comunicação diluiu as fronteiras entre níveis da guerra, colocando em causa a sua manutenção;
- a adesão ao conceito NNEC, consequência da decisão de Portugal participar na NATO Response Force (NRF), afecta os conceitos tradicionais de comando e controlo, obrigando a alterações estruturais na organização do sistema de forças.

Deste modo, optou-se por centrar a reflexão no *Impacto das TIC no Planeamento e Condução das Operações Militares*, considerando que os resultados esperados do processo de Transformação do Exército, traduzidos nos níveis de ambição constantes do Conceito Estratégico Militar, excluem “a priori” a actuação do Exército no nível operacional da guerra.

O objectivo deste trabalho e a sua questão central será, assim, determinar qual o impacto e como estão a ser utilizadas pelo Exército Português, as tecnologias de informação e comunicação, numa perspectiva de adesão aos conceitos de Guerra Centrada em Rede.

Como questões derivadas consideraram-se as seguintes:

- Qual o impacto que as TIC têm na forma de planear e conduzir as operações militares?

- De que forma afectam os conceitos tradicionais de comando e controlo?
- Quais as alterações estruturais na organização do Sistema de Forças, no ensino e treino militares que melhor poderão potenciar a sua implementação?
- De que forma se manifesta no Exército Português a adopção das novas TIC?

Para responder a estas questões optou-se por seguir a seguinte metodologia:

- Começar por caracterizar o conceito de nível operacional da guerra, através do estudo da bibliografia disponível e prospectivar a sua evolução;
- De seguida, fazer um bosquejo do que recentemente tem vindo a suceder na área das TIC, das alterações introduzidas na organização e funcionamento do Exército dos EUA e da NATO, entidades com que tradicionalmente se identifica o Exército Português;
- Projectar e propor um modelo de implementação do conceito NNEC;
- Finalmente, analisar a aplicação do modelo ao Exército Português.

Assim, no capítulo 2, ir-se-á analisar a génese do conceito de Nível Operacional da Guerra, para no capítulo seguinte, dedicado às TIC, analisar-se o que são e como evoluíram ao longo do tempo. Após uma prospectivação do campo de batalha do Séc. XXI, com base nas informações actualmente disponíveis, no capítulo 4 irá ser analisada a Revolução nos Assuntos Militares (RAM) em que nos inserimos e a resposta adoptada pela NATO, traduzida no conceito de Capacidade Centrada em Rede (NEC). Este conceito conduziu naturalmente ao de Operações Centradas em Rede (NCO) e Operações Baseadas nos Efeitos, estas últimas fora do âmbito deste trabalho. Neste capítulo far-se-á ainda uma breve incursão pelos aspectos da Liderança, atendendo a que recentemente têm surgido novas linhas de pensamento (Steven Metz), que consideram haver situações, de conflitos de baixa intensidade, em que o recurso a operações centradas em rede pode revelar-se contraproducente se não for tida em conta a primazia do factor humano e da liderança em detrimento da tecnologia.

Finalmente nos dois últimos capítulos é abordado o estágio da implementação das TIC no Exército Português bem como apresentadas algumas sugestões para a optimização da Transformação em curso, em termos de adesão ao conceito de guerra centrada em rede.

Para Apêndices e Anexos remetem-se os assuntos que servem de complemento à pesquisa e análise desenvolvidas.

## Capítulo 2 - O NÍVEL OPERACIONAL DA GUERRA

*“At the operational level your goal is not to kill the enemy, but to provide opportunities for the commander at the tactical level to kill the enemy.”*  
General Glenn K. Otis

Havendo poucos fenómenos sociais que estejam tão espalhados como a guerra, esta parece tão evidente a todos que nem sequer se pensa em defini-la, por supérfluo. Assim Proudhon escreve no princípio da sua obra, *La Guerre et la Paix*, que “*Todos fazem dela alguma ideia; uns porque a guerras assistiram, outros porque com elas contactaram, grande número porque nelas participou*” (Bouthoul, 1976, 37).

### 2.1 Nível Operacional da Guerra. A Génese do conceito

Recuando até à Grécia antiga, verifica-se que o conceito de guerra se encontra associado à estratégia enquanto “Arte do General”, referindo-se ao conjunto de manobras e batalhas que, sob o comando do “*estrategos*” (comandante-chefe), constituíam a campanha militar, conceito que se manteve inalterável até finais do Séc. XVIII. Tal como o termo estratégia, a palavra “táctica” vem do Grego “*taktikos*” e significa “colocar as coisas em ordem”.

Até ao Séc. XVII, as três ciências da guerra eram a **táctica** (como ciência de dispor os soldados na batalha e executar operações militares), a **fortificação** e a **balística**. A estratégia não tinha ali ainda lugar (Borges, 2000, 67).

Em 1770, Guibert propõe a separação da estratégia em duas abordagens: “a grande táctica” (a estratégia) e as “tácticas elementares” (a táctica). A “pequena táctica” tratava da disposição e enquadramento das unidades militares e a “grande táctica” procurava responder aos problemas associados à coordenação do conjunto de batalhas que compunham as operações militares e que obrigavam ao domínio de um conjunto alargado de competências. (Pinto, 2001).

A evolução tecnológica que entretanto se verifica e a crescente complexidade e dimensão dos conflitos existentes, estendeu estes aos domínios sociais, político e económico, retirando-os da esfera exclusivamente militar. Tornou-se então evidente a necessidade de criar um nível intermédio que explicasse a relação entre as forças, a manobra, e o uso do tempo e espaço de forma integrada, o que reintroduziu o conceito de estratégia, como “ciência do general”.

De entre os pensadores desta época destaca-se Clausewitz, que relaciona a estratégia com a táctica, considerando competir à táctica o “*ordenar e conduzir a acção nos combates*” e à estratégia “*relacionar os combates entre si, para atingir os fins da guerra*”.

Este conceito, de que a estratégia é uma combinação, mais ou menos complexa de operações tácticas é partilhada por outros pensadores, como o general Prussiano Bulow, que se destacou nas campanhas contra Napoleão e o marechal Moltke (guerra franco-alemã de 1870 -

-1871), tendo, já em pleno Séc. XX, o General Beaufre surgido com a definição mais adequada aos conflitos daquele século: “*Estratégia é a arte de empregar a força para realizar os fins da política*” (Alves, 1999, 93-96).

Já em plena revolução industrial, a revolução nos transportes, devida ao aparecimento do motor, a vapor e a explosão, associada à revolução nas comunicações decorrente da invenção do telégrafo e da telefonia, introduziram a geografia como factor a ponderar.

À medida que aumentava a dimensão do campo de batalha e a dispersão das forças, diminuía a capacidade dos comandantes para controlar as tropas e o conjunto de eventos que neles decorria. A vitória na guerra deixou de depender do sucesso de uma ou duas batalhas isoladas mas de um conjunto de combates, quase sempre dispersos no espaço e no tempo, em que o somatório de vitórias tácticas não era garantia de vitória estratégica. Na guerra da independência Americana, os Ingleses ganharam todas as batalhas que travaram no Sul dos EUA contra o general Nathaniel Green, mas o nível de baixas sofrido foi de tal modo elevado que acabaram por perder a Guerra, por exaustão dos seus recursos humanos.

A maior dimensão dos teatros de operações, a passagem da guerra limitada à guerra absoluta e a criação de escalões que passaram a agir independentemente das partes principais dos exércitos, autónomos do ponto de vista táctico e logístico (Divisões e Corpos de Exército) tornaram evidente a necessidade de um escalão intermédio entre a política/estratégia e a táctica.

A diferença básica, em relação à antiguidade, em que exércitos inferiores em número derrotaram outros muito superiores, está agora, na necessidade de conjugar a sucessão de vários choques. Para além da coordenação dos combates, parte integrante de cada batalha, passou a ser necessário coordenar as batalhas para concretizar os objectivos definidos pela estratégia.

Esta necessidade só foi reconhecida muito recentemente, já em pleno Séc. XX, pelos Estados-Maiores Alemão e Soviético, e mais recentemente pelos Estados Unidos da América em finais da década de 70<sup>1</sup>, na sequência das intervenções na Coreia e no Vietname, tendo dado origem ao conceito actual em que a guerra se considera dividida em três níveis: o estratégico, o operacional e o táctico (Fig. 1).

Assim e de acordo com a doutrina americana (FM 100-5, 1986, 9) considera-se:

- **Nível estratégico**, o que é caracterizado pelo emprego das Forças Armadas de uma nação ou aliança para alcançar os objectivos políticos através do uso (ou ameaça do uso) da força. A este nível, definem-se as condições essenciais das operações para fazer

---

<sup>1</sup> O conceito foi apresentado inicialmente por Edward Luttwak num artigo na Security International Review – Winter 1980/81 sob o título “Operational Level of War” e desenvolvido mais tarde por DAVID JABLONSKY (in *Estratégia Operacional - O Que Está para Além da Primeira Batalha*) do CF(FZ) PINTO, Rodrigues - <http://www.cgcfin.mar.mil.br>).

ou impedir a guerra. Estabelecem-se os objectivos gerais nos Teatros de Guerra e nos Teatros de Operações, atribuem-se forças, recursos e delimitam-se as condições do uso da força. A Guerra é encarada como um todo.

- **Nível tático** é aquele em que o comandante, do Corpo e das unidades de menor escalão, traduz o potencial de combate em batalhas vitoriosas. É o nível em que é feito o planeamento das operações e conduzidas as unidades em combate, de forma a atingir os objectivos militares da campanha. Neste nível, o elemento essencial é a manobra.
- **Nível operacional**, é aquele em se empregam as forças militares para realizar os objectivos estratégicos no Teatro de Guerra ou no Teatro de Operações através do **planeamento, organização e execução** de campanhas e **operações de grande envergadura**.

Deste modo, enquanto a tática se ocupa da batalha e a estratégia da guerra, o nível operacional foca-se na campanha, enquanto conjunto de batalhas. Aqui, o planeamento é feito com a preocupação de orientar as actividades táticas de modo a conseguir-se atingir os objectivos estratégicos através do confluir dos resultados das operações no conjunto do teatro de operações.

*“A chave para a delimitação entre os níveis referidos reside no facto de normalmente, a autoridade estratégica atribuir objectivos e recursos, estabelecendo as limitações necessárias enquanto que no nível operacional, o comandante define as tarefas às unidades que lhe foram atribuídas para a execução do seu próprio plano de campanha. As forças ao nível operacional têm uma dimensão que lhes permite executar operações autonomamente, e com impacto ao nível estratégico”* (NC 20-77-01, 2005, 18).

## 2.2 Nível Operacional versus Arte Operacional

Alguns pensadores referem-se indistintamente ao Nível Operacional como Arte Operacional. Outros há, que consideram nível operacional o patamar onde se desenrolam as campanhas, conjunto de batalhas e acções militares coordenadas e integradas com a finalidade de realizar objectivos estratégicos e separam o uso (nível) da forma (arte) como se empregam as forças militares, designando esta última por “Arte Operacional”. Arte Operacional é então a adição da componente humana, do carácter do comandante, ao emprego mecânico das regras e técnicas da guerra. É a arte de conjugar a tríade “tempo-espaco-forças” de forma a criar as condições para o sucesso.

Numa abordagem simplista, o nível operacional responde ao **quando**, **onde** e o **para quê** combater. Regula o emprego das forças de maior dimensão, o seu empenhamento (ou retirada) e a sequência dos combates para concretizar objectivos mais importantes.

A arte operacional, por sua vez, procura criar as condições para o comandante empregar o pessoal, material e o tempo de forma eficiente. Os chefes militares a este nível, devem ser capazes de **compreender** e **antecipar** as condições indispensáveis à obtenção da vitória no campo de batalha, de modo a só se empenharem em **confrontos necessários e decisivos**, a **reduzir perdas** desnecessárias, mas mesmo assim a alcançar os objectivos que tinham sido designados pelo nível estratégico/político.

Apesar de não existir ainda doutrina aprovada sobre este assunto, considera-se ser esta última abordagem a mais correcta, transcrevendo-se a este respeito o estabelecido no NC 20-77-01: “A Arte Operacional - Operações Conjuntas e Combinadas”:

*“Arte Operacional é o criterioso emprego das forças militares para atingir objectivos estratégicos e ou operacionais, através da concepção, organização, integração e condução de estratégias de teatro, de campanhas, de operações de grande envergadura e de batalhas. A arte operacional traduz os objectivos estratégicos num conceito operacional que, por sua vez, efectua a integração das batalhas e combates tácticos, com vista a alcançar aqueles mesmos objectivos”.*

### 2.3 O Conflito ao Nível Operacional. Guerra de Informação

Considerando que ao nível operacional é essencial compreender e antecipar as condições indispensáveis à obtenção da vitória no campo de batalha, o objectivo da guerra neste nível é influenciar a capacidade do adversário decidir de forma eficaz. É conjugar as acções ao nível operacional com as do nível estratégico de modo a conseguir-se que as decisões tomadas pelo adversário favoreçam os nossos propósitos, e simultâneamente prejudiquem a sua própria campanha (Szafranski, 2000).

A aplicação das TIC à guerra, traduz-se neste nível, na “guerra de informação” enquanto instrumento de acção sobre a epistemologia do adversário, de intervenção sobre os seus conhecimento, crenças e cultura, com a finalidade de perturbar a sua capacidade de decisão e actuação. A guerra de informação, também designada por alguns autores como guerra do conhecimento, guerra de comando e controlo ou cyber guerra, actua sobre o ciclo de tomada de decisão do adversário, procurando negar-lhe a capacidade de se ajustar e reagir adequadamente à confusão criada pela fricção e nevoeiro da guerra.

O Coronel americano John Boyd, teorizador do processo de decisão, articulou-o em quatro fases: Observar – Orientar – Decidir – Agir, conhecidas como o **ciclo OODA** (Fig. 2).

Dependendo a duração de cada fase das características pessoais do decisor, a vantagem no conflito será daquele que conseguir completar o ciclo mais rapidamente. O uso das TIC permite acelerar o ritmo da cada uma das fases mas o seu impacto é mais significativo nas fases de

**observação** e sobretudo na de **orientação**. Nesta fase, a informação recolhida durante a **observação** é processada, em conjunto com a imagem mental que o decisor tem da situação, das suas idiossincrasias e da sua cultura de modo a criar uma nova imagem, actualizada, que servirá de base para a decisão.

Para agir, há que recolher um volume de informação que seja o necessário e suficiente para se decidir de forma correcta e adequada. No ciclo da tomada de decisão, a recolha da informação necessária (mínima) para agir está associada a um “tempo” e a um esforço de pesquisa, que proporcionam uma janela de oportunidade de decisão. Para além desta, a situação de conflito corre o risco de evoluir para uma situação problemática e daí para uma situação de crise, sem que do atraso introduzido resulte qualquer vantagem significativa, em termos da qualidade quer da informação recolhida, quer de avaliação da situação (Fig. 3).

A vantagem, amplificada pela introdução das TIC, estará assim do lado do beligerante capaz de agir antes do adversário, de se lhe antecipar e de o forçar a decidir com base no conhecimento inadequado da situação, levando-o a agir de forma contrária aos seus interesses (Schetman, 1996, 34-42).

## **2.4 Evolução Futura**

A evolução das tecnologias de informação trouxe à sociedade dos Séc. XX e XXI profundas modificações tecnológicas, políticas, sociais, éticas e estratégicas. A possibilidade dos Teatros de Operações existirem simultaneamente em áreas distantes do globo, e o recurso crescente à utilização do espaço, dos satélites de comunicações e dos satélites enquanto componentes dos sistemas de armas, levou a operações dispersas no espaço e no tempo e à alteração do conceito de campo de batalha para o de “espaço de batalha”.

A crescente digitalização do espaço de batalha juntamente com a integração da informação ao nível dos Teatros de Operações provocou a diminuição drástica dos tempos de resposta e o consequente aumento da rapidez do processo de decisão, o que não é compatível com a centralização típica das organizações militares do Séc. XX. Os exércitos darão origem a unidades militares cada vez mais modulares, que manterão do passado a estrutura de comando e controlo tradicionais mas que incorporarão elementos de outros Ramos das Forças Armadas e mesmo de outros países, num formato conjunto e combinado, que será a característica dominante das operações militares futuras.

De acordo com Steven Metz, os conflitos do Séc. XXI irão assistir à alteração drástica de conceitos. Nas guerras futuras as nações não ousarão agir isoladas mas apenas quando integradas em alianças e/ou coligações. Os conflitos irão assentar em operações rápidas e decisivas. Baseando-se na superioridade de informação sobre a situação no campo de batalha, os estados

procurarão obter a superioridade de decisão, de modo a conseguir a redução de riscos e maximizar a coerência e eficácia das operações (Metz, 2000 ).

A sua mediatização, que é já um dado adquirido, irreversível, introduziu um novo paradigma, o das “baixas zero”, e fez com que as decisões tomadas aos mais baixos escalões tenham repercussões aos níveis estratégico e político, o que veio limitar a liberdade de acção dos decisores militares. Estas alterações nos cenários previsíveis da guerra terão impacto profundo na organização e estruturação das forças militares as quais serão balizadas por requisitos como:

- Modularidade,
- Menor dimensão e maior qualidade,
- Elevada mobilidade,
- Simplicidade de organização,
- Integração em estruturas conjuntas e combinadas.

Quando do estabelecimento do conceito “nível operacional” procurou-se, naturalmente, identificar os níveis de guerra em termos de espaço (Teatro de Operações) ou hierarquia de Comandos ou de Escalão (Corpo de Exército ou Exército). No período pós Guerra Fria este escalão baixou para a Brigada mas rapidamente se constatou não haver apenas um determinado escalão que possa ser considerado único responsável pelas actividades neste nível. Neste contexto, ir-se-á assistir à diluição das fronteiras entre níveis da guerra.

Esta “realidade” acaba de ter a sua confirmação na recente crise dos “cartoons”, que tendo sido publicados num pequeno jornal Dinamarquês, desencadearam uma crise mundial, em que boa parte dos actores reagem de modo violento a uma acção de um pequeno país que possivelmente nem sabe localizar.

No caso de Portugal, o nível de ambição expresso no CEM aponta para o emprego sustentado e continuado de forças de escalões (Brigada/Batalhão) que claramente se inserem no patamar táctico. Em apêndice, (Apêndice C) apresenta-se uma breve análise da incursão das Forças Armadas Portuguesas neste nível da guerra.

Precursor da realidade actual, no início do Séc. XX, o General francês Brailon considerava que *“todos os comandantes terão de em certo momento fazer estratégia, pelo que o ensino estratégico e táctico deve ser ministrado a todos os escalões de comando de modo a conferir-lhes possibilidades de intervenção no domínio da concepção estratégica, primeiro, e nos domínios da organização e execução tácticas a seguir”* (Alves, 1999, 96).

### **Síntese Conclusiva**

O nível operacional, elo de ligação entre o estratégico e o táctico, é aquele em que são desenhadas e planeadas as campanhas e operações de grande envergadura, onde são executadas e



sustentadas, de modo a alcançarem-se os objectivos estratégicos.

Considerada a necessidade do comandante operacional de “**compreender e antecipar** as condições indispensáveis à obtenção da vitória no campo de batalha, de modo a só se empenhar em **confrontos necessários e decisivos**”, a guerra a este nível, toma a forma de guerra de informação, actuando sobre a epistemologia do adversário, procurando levá-lo a tomar decisões precipitadas e/ou erradas, baseadas num conhecimento imperfeito e incorrecto da realidade.

A evolução tecnológica verificada tem vindo a esbater a separação entre níveis levando à sua sobreposição crescente. Nesta conformidade a análise do impacto das TIC irá ser considerada numa perspectiva transversal, atendendo à situação particular portuguesa e a que a sua influência se estende e interfere de uma forma global a todos os níveis.

### Cap 3 - AS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÕES

*Independentemente das dificuldades técnicas, qualquer coisa teoricamente possível, será concretizada na prática,,desde que seja suficientemente desejada.*

*Arthur C. Clark*

#### 3.1 Os Sistemas de Informação

Segundo Steve Alter, Sistemas de Informação (SI) são “*a combinação das componentes, métodos de trabalho, informação, pessoas e Tecnologias da Informação e Comunicações, organizados de modo a atingir os objectivos organizacionais*” (Pinto, 2004) .

Mais que os sistemas informáticos, a que ainda frequentemente se associam, são a componente da organização responsável pela recolha, tratamento, armazenamento e distribuição da informação relevante para a mesma. Têm o propósito de facilitar o planeamento, o controlo, a coordenação, a análise e a tomada de decisão.

O elemento base dos SI são os **dados**, conjuntos de elementos discretos, não organizados, compostos por números, palavras, sons ou imagens independentes, e que podem ser facilmente estruturados. Sendo úteis para o desempenho de uma determinada tarefa, só servem para a adopção de uma acção ou apreensão de uma situação após terem sido devidamente trabalhados.

Quando trabalhados, e a sua estrutura se torna adequada para utilização, está-se perante **informação**, a qual pode ser usada pelo processo de decisão.

Finalmente, conhecimento é a informação associada a uma experiência, que compreende uma estratégia, uma prática, um método ou uma abordagem (Dinis, 2005,23).

Os elementos constantes num Sistema de Informação são assim o **produto** (dados e informação armazenados), a **tecnologia dos processos** (equipamentos), a **tecnologia do produto**

(aplicações), a **organização** (procedimentos, normas e estratégias organizacionais) e pessoas (que analisam e decidem com base nos SI) (Dinis, 2005, 24).

Sendo sistemas dinâmicos, caracterizam-se por serem motor de mudança nas pessoas, organizações e tecnologias, visando, acima de tudo optimizar o processo de decisão (Fig. 4).

### 3.2 A Evolução dos Sistemas de Informação

Os anos 70 assistiram à adopção das TIC pela sociedade em geral, e ao desabrochar da “sociedade de informação”. A evolução rápida e acentuada dos SIC pulverizou distâncias, estilhou fronteiras e aproximou as pessoas, dando origem à “aldeia global” de Marshall MacLuhan (Nyer, 2002, 266). Os Sistemas de Informação passaram de processadores quantitativos de informação estatística (financeira, logística e de pessoal) a sistemas qualitativos, de apoio à decisão.

Influenciaram drasticamente as empresas e organizações, através do incremento da partilha de recursos, do intercâmbio de informação, da inovação e normalização de processos, num processo bi-direccional que levou ao reajustamento das estruturas organizacionais e respectivas culturas, as quais por sua vez obrigaram a novas evoluções nos sistemas, num ciclo que se repete até hoje (Fig. 5).

A evolução dos SI fez-se em quatro fases, que correspondem a etapas na evolução tecnológica, iniciando-se nos processadores de dados, passando pelos microprocessadores até chegar às redes, dependendo das diferentes utilizações dos SI, e do ênfase ser colocado no processamento ou na partilha de dados (Rodrigues, 2002, 3):

- **Automatização**, ou seja substituição do trabalho manual por soluções tecnológicas, baseada no processamento de dados, com o apogeu entre 1960 a 1980, e em que os SI são do tipo transaccional, orientados para processar grandes volumes de dados e registar as transacções diárias necessárias à condução da organização;
- **Informação**, em que a tónica é posta na ampliação da capacidade humana para processar informação e concide com a introdução dos microprocessadores nos finais da década de 70, princípio da de 80. É a fase dos Sistemas de Informação de Gestão (Management Information Systems - MIS), orientados para o apoio às actividades de gestão das empresas e, de forma incipiente, à tomada de decisão;
- **Incorporação**, sobreposta no tempo ao período anterior, visando a substituição de controlos, mecânicos e electromecânicos, por microprocessadores. Permitiu novas formas de aquisição, partilha de dados e novas funcionalidades, coincidindo com o desenvolvimento dos microprocessadores;
- **Comunicação**: tirando partido da evolução das comunicações teve por fim melhorar a

partilha de informação, através das redes informáticas. É o período dos anos 90 e dos sistemas de apoio à decisão, (Decision Support Systems), concebidos especificamente para apoio ao processo de tomada de decisão, com capacidades analíticas avançadas, e desenhados à medida dos utilizadores.

Estas fases correspondem por sua vez a três “eras” de crescimento e maturidade dos SI, como descrito por Mutsaers (1997), que considerou que os SI passam pelas “eras” de: *Processamento de Dados* (PD), *Tecnologias de Informação* (TI-Microprocessadores) e *Redes* (R) como se descreve na Fig. 6. Cada era inicia-se por um período de *evolução*, seguido por um de *estabilidade* culminando com um período de *descontinuidade* antes de se iniciar uma nova era, sendo esta descontinuidade uma revolução mais do que uma transição evolucionária (Rocha, 2002, 17).

Até meados dos anos 90, todos estes sistemas estavam geograficamente dispersos e as trocas de informação entre eles eram reduzidas, não se tirando partido da sua potencial ligação em rede. Para poderem comunicar entre si, os sistemas tinham de se ligar e sincronizar, no tempo e no espaço, e só depois podiam proceder à troca de informação.

Face à redução de custos associada ao progresso tecnológico, assistiu-se a uma progressiva aposta na “força bruta” do processamento. Esta tendência teve por base a constatação de que a capacidade de armazenamento de informação num circuito integrado duplica a cada 18 meses, a preço constante, de acordo com a Lei de Moore<sup>2</sup>.

No entanto, os avanços que se seguiram nas tecnologias das comunicações, com a largura de banda dos sistemas a triplicar em cada 12 meses (Lei de Gilder, 1997) originaram uma nova inflexão nos SI. Assistiu-se à explosão das redes de computadores e ao aparecimento e consolidação da Internet e das ferramentas de partilha de informação como o correio electrónico e os motores de busca ou “browsers” (Anexo A).

O correio electrónico, eliminou a necessidade de sincronismo prévio entre sistemas fisicamente separados, se bem que se mantivesse a necessidade de o originador da informação saber para quem, e qual a informação a enviar. Paradigmático desta fase é o sistema LOCE<sup>3</sup>, de origem americana, adoptado pela NATO e muito apetezido pelos analistas de informação, pela sua capacidade de fornecer um serviço de correio electrónico NATO SECRETO.

Por sua vez, as redes e mais especificamente a Internet (www) levaram a uma inversão dos modelos baseados na suposição Smithsonianiana de que o ser humano é egoísta e avesso à partilha. O novo paradigma empresarial é hoje “partilhar” a informação, conhecimento e tecnologia,

---

<sup>2</sup> Lei de Moore: a capacidade de um circuito integrado =  $2^t$  (t-1962), sendo t a data actual, em anos.

<sup>3</sup> LOCE : Linked Operational Intelligence Centers Europe.

tendo-se verificado que os maiores avanços nos últimos anos aconteceram em áreas de conhecimento como a nanotecnologia e a economia comportamental, precisamente com base na cooperação de especialistas de diferentes áreas de saber. O prémio Nobel da economia de 2005, foi atribuído a Thomas Schelling em parte pela sua demonstração de que as pessoas tendem a desenvolver trabalho colaborativo muito mais do que o previsto pelos modelos económicos tradicionais. Yochai Benkler, professor de economia em Yale, considera que se está perante uma inflexão dos modelos organizacionais do passado, de estruturas hierarquizadas, para um novo modelo organizacional a que chamou “*the new networked information economy*” (Foroohar, 2005, 40-41).

Com a ligação rotineira em rede dos diferentes SI, a partilha de informação que se caracterizava pelo “push”, base do correio electrónico, e que obrigava o produtor de informação a conhecer as necessidades do utilizador final, passou para um sistema de “pull”, graças aos motores de busca disponibilizados pela Internet e à consequente alteração cultural a eles associada.

Hoje, os fluxos de informação militares da NATO caracterizam-se pela criação de repositórios de informação, de onde os utilizadores finais (comandos NATO, países ou outros CIS devidamente autorizados) a vão retirar (pull), com base na sua necessidade de conhecer (AC/322 WP 0002 de 1Abr2005). Precursor desta alteração foi a transformação do NACCIS<sup>4</sup> em MCCIS<sup>5</sup> com a adopção de tecnologia Web, nos finais da década de 90.

No futuro, espera-se que a nanotecnologia possibilite manipular átomos e moléculas individuais de modo a construir “máquinas” mecânicas, eléctricas e biológicas que irão substituir muitas das ferramentas e processos usados hoje em dia. Aplicada aos computadores, esta tecnologia irá provocar o aparecimento de novas gerações de equipamentos cada vez mais potentes e de menores dimensões, que por sua vez irão provocar e acelerar novos avanços na tecnologia, numa escala que pode ser antecipada apenas em ordem de grandeza e que levará a globalização ao seu extremo.

Muitos analistas acreditam que a Lei de Moore continuará a ter aplicação até cerca de 2020. Considerando-se que os computadores mais recentes têm mais de 40 milhões de transistores, calcula-se que em 2015 poderão ter cerca de 5 biliões. Estas novas máquinas terão capacidades incomensuravelmente superiores às actuais e poderão dar origem a sistemas inteligentes autónomos, prevendo Ray Kurzweil que em 2020 se assistirá a uma nova descontinuidade, precursora de nova Revolução nos Assuntos Militares, com os computadores a

---

<sup>4</sup> NACCIS – North Atlantic Command and Control Information System

<sup>5</sup> MCCIS – Maritime Command and Control Information System

tornarem-se, finalmente, mais inteligentes que o Homem (Petersen, 2002, 2-4 ).

### 3.3 As Revoluções nos Assuntos Militares

Em contraponto a Heidi e Alvin Toffler, Andrew Marshall, director do Office of Net Assessments do gabinete do Secretário da Defesa dos EUA, considera “*Revolução nos Assuntos Militares - RAM*” como “*uma alteração de grande envergadura na natureza da guerra, provocada pela aplicação criativa de **novas tecnologias** que, em conjunto com **alterações na doutrina** militar e nos **conceitos operacionais** e **organizacionais**, modifica drasticamente o carácter e a condução das operações militares*” (Tilford, 1995, 1).

No campo militar, as Tecnologias de Informação e Comunicação introduziram alterações profundas ao nível da compressão do espaço/tempo e da criação de um mundo sem fronteiras, conduzindo a uma verdadeira revolução no modo de conduzir a guerra (Anexo B)

A RAM em que nos encontramos aposta na integração de sistemas, assentando na conjugação de vários sistemas de armas diferentes, encarados sob novas perspectivas e utilizados de forma inovadora para criar um efeito final revolucionário. Segundo Steven Metz, esta RAM caracteriza-se, face ao passado, por quatro tipo de alterações (Metz, 1995, 7-12):

- Ataques precisos, com recurso a munições com guiamento de precisão;
- Avanços dramáticos no comando, controlo, comunicações e informação (C3I);
- Ênfase na guerra de informação;
- Preocupação com a não letalidade;

Trata-se de uma RAM de “sistema de sistemas”, resultado dos desenvolvimentos técnicos, organizacionais e sócio-económicos verificados nos recentes anos, que procura tirar partido do efeito acumulado do emprego simultâneo e integrado das novas capacidades à disposição do aparelho militar e que cobre a totalidade do teatro de operações. Na Fig. 7 apresenta-se a relação entre os conceitos operacionais, modelos de actividade operacional e tecnologias associadas, mostrando o peso que as tecnologias de informação têm neste processo.

No passado, tem havido, em regra, um desfazamento de décadas entre a disponibilização das tecnologias para uso civil, comercial, e o seu aproveitamento para fins militares<sup>6</sup>. Na área das TIC, porém, verificou-se a adesão imediata dos novos parceiros na cena internacional, (estados falhados, grupos terroristas, organizações criminosas transnacionais), às novas tecnologias.

Assentando as inovações em produtos comerciais (COTS<sup>7</sup>), não precisam concentrar recursos em programas de investigação e desenvolvimento complexos e dispendiosos, mas tão só

---

<sup>6</sup> Caso da utilização do caminho de ferro pelo exército prussiano de von Moltke, em 1860, e da “blitzkrieg” pela Alemanha do 3º Reich com base em tecnologia datada da IGM.

<sup>7</sup> COTS: Commercial of the Shelf

de integrar e aplicar tecnologias existentes no mercado. Tecnologias que podem ser adquiridas aos produtores que estejam na vanguarda tecnológica, o que aumenta o grau de imprevisibilidade do campo de batalha futuro. Por outro lado como as infraestruturas em que assentam as sociedades ocidentais são extremamente dependentes destas mesmas tecnologias, aumenta exponencialmente o risco a que as sociedades desenvolvidas estão sujeitas.

Uma outra lição do passado a ter presente é a de que só se consegue tirar rendimento do potencial proporcionado por uma nova tecnologia quando, concomitantemente, se procede à adaptação da organização receptora e respectivos processos de negócio (Fig. 8).

### **3.4 A Implementação das RAM. O Modelo YETTON**

O modelo YETTON<sup>8</sup>, é um modelo que pode ser usado para analisar a introdução de novas capacidades nas empresas e em estruturas militares.

Segundo este modelo (Fig. 9), a introdução de uma nova capacidade, inicia-se pela análise e reajustamento da estrutura que irá incorporar essa capacidade. Esta alteração induz alterações nos processos o, que por sua vez obriga ao desenvolvimento de novos requisitos de recrutamento, formação e treino das pessoas. Só depois se procede à introdução da tecnologia que possibilitará o fornecimento da nova capacidade. O processo é sujeito a sucessivas iterações, que usam a experiência dos utilizadores para conseguir uma melhoria constante dos procedimentos, mas sempre dentro da mesma estrutura (Potts, 2003, 33-35).

Quando se está perante uma RAM, o modelo sofre uma inflexão e a adopção de novas capacidades, baseadas em tecnologias de ponta, começa pelo envolvimento das pessoas com visão para criar uma nova estrutura capaz de rentabilizar a capacidade em causa. O processo inicia-se pela introdução da tecnologia e o levantamento da nova estrutura. Esta irá então forçar a adopção de novos processos e permitir a exploração da nova capacidade. A diferença, é que agora, é primeiro implementada a capacidade e só depois rentabilizada, estando todo o processo dependente da capacidade de liderança/influência dos indivíduos com a visão revolucionária inicial (Fig. 10).

### **3.5 O Campo de Batalha do Sec XXI**

Segundo Arthur C. Clark, *“uma leitura crítica da ficção científica é um treino essencial para qualquer pessoa que pretenda olhar a mais de dez anos de distância no futuro”* (Clark, 2001, 17).

Na 1ª Guerra do Golfo, entre a identificação e o bombardeamento de um alvo existia um intervalo de três dias, porque as ordens tinham que ser encaminhadas para os porta-aviões. Já

---

<sup>8</sup> Philip Yetton é professor da Australian Graduate School of Management.

em Abril de 2003, entre a informação de que Saddam Hussein estava em reunião com comandantes militares de topo e o momento em que um bombardeiro B-1B lançou quatro bombas de 2000 libras guiadas por satélite sobre o local referenciado, decorreram apenas 45 minutos (Boot, 2003, 52).

Prospectivando esta evolução e face à democratização do acesso às tecnologias de ponta (função do custo decrescente e simultaneamente da sua disponibilidade no mercado), o campo de batalha em meados do Séc. XXI será imprevisível, pontuado de conflitos assimétricos, com configurações atípicas, *“habitado por drones e armas inteligentes”*. O paradigma do Séc. XX, do combate em que os contendores se enfrentam cara a cara dará lugar a um mundo onde os combatentes estarão escondidos por trás de sofisticados equipamentos de controlo remoto, tendo à sua disposição sistemas de informação revolucionários.

Este campo de batalha caracterizar-se-á pela elevada mobilidade e iniciativa das forças que nele evoluem, por frentes irregulares, pelo aumento da letalidade e do poder de fogo e sobretudo pela complexidade dos aspectos políticos e da envolvente tecnológica de que se revestirão os conflitos. A superioridade de informação no conhecimento da situação do campo de batalha será fundamental. (Vaz, 2004, 98-102).

Neste ambiente será fulcral dispor dos melhores meios de recolha de informação, com recurso crescente aos UAV (Unmanned Aerial Vehicle) e às actividades ISTAR (Intelligence, Surveillance, Target Acquisition and Reconnaissance).

### **Síntese Conclusiva**

Na Sociedade de Informação, a informação tem um efeito multiplicador que dinamiza todos os sectores e constitui o motor do desenvolvimento político, económico, social e tecnológico. As vantagens competitivas passaram a ser obtidas através da utilização das redes de comunicações e dos SI que interconectam os diferentes parceiros estando-se a verificar uma alteração de paradigma no sentido da “partilha” de informação e do conhecimento.

Atendendo a que os adversários têm acesso à mesma tecnologia e armamento, o elemento da diferença, que pode proporcionar a vitória, será a rapidez e eficácia com que se implementam estruturas da era da Informação, em particular as que incentivam a “partilha” da informação, sejam elas Sistemas de Informação, sistemas de simulação ou de treino conjuntos.

A difusão quase instantânea da informação está a alterar as formas tradicionais como as organizações se estruturam e operam, eliminando níveis de decisão intermédios. No entanto estas alterações, dado o seu carácter revolucionário, só serão efectivas se impulsionadas por líderes com visão, iniciativa e domínio efectivo sobre as organizações.

## Capítulo 4 - IMPACTO DAS TIC NAS OPERAÇÕES

*One can not manage change. One can only be ahead of it  
Peter Drucker*

### 4.1 Sistemas de Comando e Controlo e o Processo de Decisão Militar

A introdução dos modernos sistemas de comando e controlo e a alteração no processo de decisão militar foram duas das mais significativas alterações introduzidas pelas TIC na forma de planear e conduzir as operações militares.

Até à I Guerra do Golfo, os relatórios de situação eram enviados por rádio e a situação das forças, amigas e inimigas, registada nos transparentes de situação, em folhas plásticas, com lápis stencil. Hoje os sistemas de comando e controlo permitem visualizar a situação das forças em ecrãs digitais nos postos de comando da maior parte dos exércitos ocidentais. Da visualização parcelar da situação das próprias forças e das do inimigo, passou-se para a observação em tempo real da Common Operational Picture (COP) que permite ao comandante da força saber em qualquer instante, não só onde se encontra mas mais importante ainda, onde estão as forças amigas e as inimigas, sejam elas terrestres, navais ou aéreas.

O processo de planeamento militar, de sequencial e concorrente, passou a ser feito de forma cooperativa e interactiva, pelo comandante e pelo seu Estado Maior, graças às ferramentas e facilidades proporcionadas pelos sistemas de Comando e Controlo (C2) e pelo uso generalizado das redes e sistemas informáticos.

Elementos cruciais deste processo são a definição da missão e intenção do comandante, a sua directiva inicial de planeamento bem como os seus requisitos críticos de informação. Este conjunto constitui a pedra angular do futuro paradigma de liderança e de descentralização da decisão.

### 4.2 Os novos Paradigmas da Guerra

Segundo o TGen Garcia Leandro *“estamos já num mundo novo, numa nova era, de barreiras abatidas, de perda de poder dos Estados e das empresas da Era Industrial, onde quem domina a informação e as novas tecnologias terá o poder”* (Dinis, 2005, 12).

Com o fenómeno da globalização e o advento da Sociedade de Informação, surgiu um novo tipo de ameaça, caracterizado por ter na sua origem organizações não estatais, caracterizadas por um grau elevado de incerteza quanto aos objectivos, motivação e capacidades. Alteraram-se os centros de gravidade da distribuição de poder, ao mesmo tempo que as distâncias e a geografia perderam a importância e o peso tradicionais.

Mesmo conflitos inicialmente enquadráveis na tipologia da guerra clássica, como a recente invasão do Iraque, rapidamente se transformam em conflitos atípicos, assimétricos, com um



lado a usar técnicas e táticas convencionais, com recurso ao uso limitado da força, face a um adversário que usa todos os meios ao seu dispor, sem nenhuns constrangimentos.

O conceito de ameaça encontra-se em plena transformação, tendo passado a ser mais difusa e diluída e ao mesmo tempo transnacional o que conduz à tendência para a diminuição da intensidade da coacção militar. Está-se perante um modelo de conflito, onde o Estado perdeu o monopólio da violência e o aspecto fulcral é a partilha da informação e do conhecimento.

Os Sistemas de Informação de Comando e Controlo foram o instrumento desta alteração, tendo criado condições, como nunca antes conseguidas, para a redução drástica do tempo de decisão, a economia de forças, a redução do fratricídio e o apoio logístico eficiente e atempado. Do modelo corporativo de partilha de informação, entre Comunidades de Interesse (COI) passou-se para um modelo co-operativo, partilhado, onde a informação está ao alcance de quem dela necessita (Fig. 11).

#### 4.2.1 NCW / NNEC

Nos anos 90, na sequência das guerras do Golfo, surgiu um novo conceito de guerra, que procura rentabilizar, de forma exponencial, os princípios da economia de forças, surpresa e unidade de comando.

Baseia-se na obtenção da superioridade de informação e partilha dessa mesma informação por todos os componentes da força, conjugada com o seu emprego sincronizado, de modo a obter uma vantagem decisiva no local e momento adequados.

Tal como sucedeu com a teorização do nível operacional da guerra, iniciado após a II GM, os novos paradigmas e os conceitos associados só muito recentemente começaram a ser objecto de estudo e análise. O conceito foi apresentado pelo Almirante americano Jay Johnson num seminário no Naval Institute Annapolis, em 1997. O Almirante Johnson considerou estar-se perante uma RAM caracterizada pela mudança da guerra centrada na plataforma (*platform-centric warfare*) para um nova forma de guerra, desta vez centrada na rede de plataformas, de unidades, e de forças (NCW: *network-centric warfare*)<sup>9</sup>.

Segundo o Almirante Johnson, a NCW assenta nas seguintes premissas :

- uma força organizada em torno de uma estrutura em rede, melhora drasticamente a sua capacidade de partilhar informação;
- a partilha da informação e a cooperação entre os diferentes elementos reforça a qualidade da informação em circulação e a percepção da situação operacional;

---

<sup>9</sup> Este conceito deu por sua vez origem nos EUA, respectivamente aos conceitos de Navy Cooperative Engagement Capability (CEC), da Air Force Expeditionary Force e da Army Force 21.

- a crescente percepção, partilhada, da situação operacional possibilita a auto sincronização entre os diferentes componentes;
- a sincronização entre as partes aumenta a eficácia do conjunto e do cumprimento da missão;

A guerra centrada em rede (Network Centered Warfare) parte da existência de forças dispersas, que tiram partido das TIC para garantir a ligação e partilha constante de conhecimento, o que lhes dá a capacidade para aumentar extraordinariamente o ritmo das operações. Deste modo conseguem reduzir a sua duração, diminuir os riscos e rentabilizar ao máximo o uso da força (Cebrowski, 1998, 5).

Actuam à semelhança de um enxame, em que as forças (modulares) evoluem, dispersas, mas se reúnem rapidamente para desferir o golpe decisivo e em seguida tornar a dispersar, negando ao adversário a possibilidade de reacção. A dispersão geográfica, aliada ao uso intensivo das TIC permite a concentração de efeitos, torna o apoio logístico mais facilitado e nega ao adversário alvos remuneradores.

No “Joint Vision 2020”, documento que permite aquilatar da importância deste conceito, as Forças Armadas Americanas assumem claramente a importância da superioridade de informação, factor multiplicador da força, para lidar com conflitos futuros.

Este documento considera serem as TIC o motor de evolução e apresenta uma visão conjunta da utilização das Forças Armadas, definindo como requisitos para obter a superioridade em todo o espectro de conflitos:

- a integração das forças e capacidades de modo a que o produto final seja maior que o somatório dos efeitos de cada parcela considerada individualmente;
- alterações na organização e doutrina, como consequência das inovações tecnológicas;
- obtenção de superioridade decisiva na utilização das modernas tecnologias<sup>10</sup>;
- garantir a maior qualidade no recrutamento, instrução e treino dos combatentes;
- garantir a interoperabilidade com outras organizações internacionais (IO) e organizações não governamentais (ONG), que estejam presentes nos TO;

Por sua vez, a NATO aderiu a este conceito e em Nov2002, o NC3Board iniciou o desenvolvimento do conceito NATO da capacidade de operar em rede (NNEC), na linha do pensamento americano.

A NNEC é um conceito estruturante da capacidade militar da NATO e visa conseguir esta capacidade através do levantamento e sustentação de forças conjuntas, “*net centric*”, capazes de,

---

<sup>10</sup> Atendendo a que os adversários terão fácil acesso às mesmas.

partindo da superioridade da informação, obter a superioridade de conhecimento e de decisão para alcançar a superioridade de efeitos (Fig. 12).

Trata-se de um conceito de operações militares proporcionado por uma superioridade no acesso, na partilha e na segurança das informações, que gera um aumento do potencial de combate, pela ligação em rede de sensores, decisores e executantes, *“de modo a alcançar grande rapidez de decisão e maiores ritmo de operações, letalidade, capacidade de sobrevivência e sincronização, transformando a superioridade na área das informações em poder de combate”* (Santos, [www.jornaldefesa.com](http://www.jornaldefesa.com)).

Regressando ao ciclo de tomada de decisão de John Boyd, está-se perante um conceito que depende da maximização da capacidade de decisão, de manipulação do ciclo OODA e da capacidade de liderança dos decisores. Em anexo (Anexo C) apresentam-se exemplos da introdução deste conceito nas Forças Armadas Alemã, Francesa e Britânica.

#### **4.2.2 - Modelos Lógico e Físico**

Os conceitos NCW e NNEC assentam numa arquitectura em 3 patamares, ligando em rede sensores, decisores e executantes, arquitectura (Fig. 13) que “vê” as forças não como entidades individuais, mas como componentes de um conjunto, que contribuem para o resultado final.

A rede de sensores recolhe e passa a informação aos sistemas de comando e controlo da infraestrutura de informação, onde é criada a compreensão da situação a qual é então acedida pelos decisores e pelos sistemas de armas. Com uma aposta muito forte na qualidade superior dos sistemas de comando e controlo pretende-se reduzir o tempo que leva a informação a fazer o circuito sensor-decisor-executor e conseguir assim a vantagem decisiva na execução das operações. O objectivo é usar a informação como factor exponenciador do potencial de combate e da eficácia no cumprimento da missão.

O conceito “centrado em rede” é o cimento que integra os domínios da guerra (físico, da informação e cognitivo) com os requisitos de superioridade de informação, superioridade de conhecimento e superioridade de decisão, para se atingir a superioridade nos efeitos finais (Fig. 14). Pretende-se que o conceito evolua para um sistema de elementos em que os vários subsistemas, desde os sensores e sistemas C2 até aos sistemas de armas, possam ser seleccionados individualmente de forma a construir sistemas de armas virtuais, “montados” à medida e formato que melhor sirva o propósito da missão (Walker, 2005, 36-37).

A noção base é considerar cada sensor, sistema C2, sistema de armas e cada plataforma como um elemento individual, identificado pelo seu endereço IP, os quais poderão ser agrupados num sistema de armas “virtual”, em que, no limite, a plataforma dispara não só sem intervenção do operador mas ainda sem que este de tal tenha consciência prévia (Fig. 15).

#### 4.3 A Transformação das Forças Terrestres. Implicações nos domínios da guerra

A implementação do conceito NCW, enquanto aquisição de uma “**capacidade em rede**”, passa pela actuação ao nível das componentes de qualquer Capacidade: Pessoas, Processos, Organizações e Tecnologia (Garstka, 2005, 6).

Relacionando estas componentes com os domínios de intervenção da NCW, é possível construir-se um modelo para análise da transformação das forças à luz deste conceito (Fig. 16). A sua implementação, traduz-se assim **ao nível físico**<sup>11</sup>, pela:

- organização modular das forças;
- criação de uma info-estrutura que :
  - disponha de um sistema de comunicações com largura de banda adequada ao volume dos fluxos de informação esperados;
  - Garanta a segurança e resiliência das infraestruturas de comunicações (redes);
  - Garanta a interoperabilidade entre os diferentes sistemas existentes no espaço de batalha.

No **nível da informação**, há que definir:

- procedimentos<sup>12</sup> e doutrina conjunta, de modo a garantir a acessibilidade da informação;
- uma política de gestão de informação<sup>13</sup>, que garanta a sua coerência e relevância.

Aos **níveis cognitivo e social**, o conceito NCW dará origem ao “*militar do conhecimento*” segundo Peter Drucker, em contraponto ao “*militar manual*” do Séc. XX, para o que:

- haverá que mudar a cultura militar para ter carácter conjunto, com ênfase na partilha de informação;
- se deverão ajustar os processos de recrutamento, selecção, formação e treino de molde a ajustar os modelos de liderança à nova realidade.

Finalmente, há ainda a considerar a **interoperabilidade** entre todos os intervenientes e o relacionamento com a indústria, passando-se de um modelo de desenvolvimento e de aquisições orientado para a quantidade, para um modelo baseado na qualidade e empregabilidade em ambiente NCW.

##### 4.3.1 A infoestrutura de Informação

Condição essencial à implementação dos conceitos referidos, é a existência de uma infraestrutura<sup>14</sup> de suporte, a Global Information Grid (GIG) dos EUA ou a NNEC-NII<sup>15</sup>,

---

<sup>11</sup> Da actividades de recolha, transporte, tratamento e disseminação da informação bem como da sua aplicação por intermédio do sistema de forças.

<sup>12</sup> Para a captura, fusão, processamento e divulgação da informação.

<sup>13</sup> Que passa pela existência de entidades/órgãos responsáveis pela gestão e pela coerência da informação.

organizada em torno das seguintes componentes essenciais:

- Serviços de comunicações;
- Serviços de integração de informação;
- Segurança da informação;
- Serviços de gestão e controlo;

à qual se ligam os elementos operacionais (Comandos NATO, QG multinacionais, etc) a fim de receber e fornecer informações (AC/322-SC/1WP004, 30Jun05, 2-5).

A info-estrutura será constituída por um núcleo duro, a “infraestrutura de base” que interligará os CIS dos elementos operacionais, sendo este núcleo duro (CCI<sup>16</sup>) formado por uma rede de redes que procurará responder aos requisitos de informação das forças. A construção desta info-estrutura levanta no entanto problemas ao nível de:

- Construção de sistemas CIS robustos, seguros e fiáveis, face aos elevados custos associados;
- Estrutura de gestão destes sistemas, necessariamente centralizada, transversal aos Ramos e que terá de resolver as rivalidades corporativas existentes;
- Estabelecimento e implementação de políticas comuns de segurança de informação;
- Formação e treino dos utilizadores e operadores, para o que se deverá dispor de sistemas de simulação adequados;
- Certificação dos sistemas, garantia de interoperabilidade e interconectividade com outros sistemas.

O envolvimento das indústrias de defesa nacionais é determinante para o sucesso da implementação deste conceito. Há que estabelecer verdadeiras parcerias entre a componente militar e a Indústria na área das novas tecnologias, uma vez que o sucesso em futuros conflitos estará dependente da incorporação e controlo das TIC, bem como das nanotecnologias e da robótica num futuro próximo.

Infelizmente, o esforço de modernização debate-se com problemas orçamentais que condicionam a transformação das forças. Face à ausência de uma ameaça percebida pela opinião pública, o critério primordial da transformação é esta ter um custo aceitável para os orçamentos nacionais. Mais uma vez a partilha, agora de custos, pode ser a solução para o problema, através da participação em programas multinacionais de desenvolvimento e de interoperabilidade.

Um exemplo é o da solução encontrada nos Estados Unidos, em que o Exército e o Corpo

---

<sup>14</sup> A que se chamará, indiferentemente, info-estrutura.

<sup>15</sup> NNEC-NII : NNEC Networking Information Infrastructure.

<sup>16</sup> CCI : Core CIS Infrastructure.

de Fuzileiros decidiram racionalizar os seus sistemas adoptando o FBCB2<sup>17</sup> do Exército para Brigada e escalões subordinados e o C2PC<sup>18</sup> dos Marines para os escalões Brigada e superiores. Com esta decisão, normalizaram equipamentos e conseguiram obter uma gestão mais optimizada da Largura de Banda existente, um bem escasso e muito apetecido pelo mundo empresarial civil.

#### **4.3.2 Gestão da Informação**

O objectivo da NNEC é a criação de um ambiente que interligue pessoas, sistemas, infraestruturas e processos em rede, e suporte uma partilha efectiva de informação, ao mesmo tempo que garanta a gestão dessa informação e a gestão do conhecimento subjacente (NNEC Data Strategy, 2004, 6-10).

Um dos problemas a resolver é o da existência de inúmeros originadores/produtores de informação, cada um com o seu sistema de informação, regra geral não compatíveis entre si, da existência de dados com estruturas, locais e repositórios de armazenamento diferentes. Para se conseguir passar de trocas de informação ponto-a-ponto, entre sistemas heterogéneos, para uma situação de partilha de muitos-para-muitos, há necessidade de pôr ordem neste ambiente.

Este desiderato exige uma entidade gestora da coerência dos dados, de forma a garantir que estes tenham o mesmo significado para todos, sejam capturados apenas uma única vez e possam ser usados indefinida e indiscriminadamente por todos os SI. Trata-se de criar uma entidade que se responsabilize pela gestão e controlo dos dados em termos da sua identificação, controlo, manipulação e arquivo, e da sua disponibilização num espaço comum, partilhado. Os seus objectivos principais serão aumentar o volume de dados disponibilizados à comunidade de utilizadores deste ambiente de rede e garantir que estejam num formato que possa ser usado por todos os utentes e aplicações.

Estamos perante uma mudança de paradigma na gestão de informação com profundas implicações nas organizações. Do “processar, explorar, disseminar” passa-se para o “disseminar antes de processar”. Os utilizadores e aplicações com os devidos acessos e autorizações terão acesso imediato à informação existente na rede, sem os atrasos e demoras inerentes ao antigo paradigma, ficando à sua responsabilidade a interpretação dos dados assim disponibilizados.

Esta nova abordagem cria a necessidade de se resolverem os problemas de interoperabilidade entre sistemas e aplicações e alerta para a inexistência de meios suficientes, leia-se de sistemas de recolha de dados e de largura de banda adequada, para a disseminação dos

---

<sup>17</sup> FBCB2: Force XXI Battle Command Brigade and Below, sistema que disponibiliza a imagem da “situação” do campo de batalha desde o nível Brigada até ao combatente individual.

<sup>18</sup> C2PC: Command and Control Personal Computer, Information System.

grandes volumes de dados que estarão em causa nos conflitos do futuro.

#### 4.3.3 Conjunto/combinado

A tendência do futuro serão umas Forças Armadas assentes numa perspectiva conjunta e com um modelo de organização modular e flexível. Esta perspectiva de **Conjunto**, segundo o General Vaz Afonso, ex-CEMFA<sup>19</sup>, é um estado de espírito que “*requer mais hábito que estrutura orgânica*” e assenta :

- No **ensino** das suas potencialidades, proporcionado por um sistema de ensino comum;
- Na **tradição** que se consolida, com o passar do tempo;
- No **hábito** que se adquire e consolida com o treino, prática e aprendizagem fornecida pela participação em exercícios conjuntos.

Assim, o grande desafio a vencer é, em tempo de paz, conseguir criar a mentalidade conjunta que irá permitir integrar no espaço de batalha forças dos três Ramos.

Face à evolução tecnológica que está a condicionar a actual RAM apontando para Exércitos à base de “Unidades Digitais” põe-se a questão de saber se Portugal quer, e pode, acompanhar este conceito evolutivo e ser capaz de participar em operações conjuntas e combinadas onde este nível de exigência é enorme. A este respeito, diz Telo (2003):

*“No actual contexto de partilha de soberania, a capacidade de participação de qualquer estado só vai até onde alcançar a sua efectiva capacidade de participar em operações combinadas. (...) Um estado que não se faça ouvir, num nível superior de decisão, tem a sua soberania limitada e amputada.”*

#### 4.3.4 Comando e Controlo versus Liderança

O conceito de operações centradas em rede assenta na crença de que a partilha da informação conduz à superioridade de informação, esta à superioridade de decisão, e daí ao incremento da eficácia da força. Os fluxos de informação mudam. Deixam de ser verticais, segundo a cadeia de comando e passam a ser não só verticais mas também transversais.

Porém este fluxo quase ilimitado de informação comporta em si riscos a ponderar para se evitarem as consequências do “paradoxo da abundância” (Nye, 2002, 253) que pode levar à paralisação, porquanto o excesso de informação poderá :

- Sobrecarregar o comandante e o seu Estado Maior, dificultando e atrasando o processo de decisão;
- Impossibilitar a destrição entre a informação relevante e a que constitui mero “ruído”;
- Conduzir a que os comandantes dos escalões superiores, tendo acesso à mesma ou a

---

<sup>19</sup> Painel no IESM em 23Jan2006

mais informação que os comandantes subordinados, cedam à tentação de fazer a microgestão das actividades destes, interferindo na execução;

- Levar a que os comandantes se concentrem no controlo das operações, em detrimento do comando efectivo das suas forças, ficando a aguardar pela última actualização (que está sempre para chegar) para então decidir.

Está-se perante uma revolução cultural, que exige dos comandantes capacidade para lidar com fluxos maciços de informação sem negligenciar a chefia e liderança dos seus homens na batalha. Com a disponibilização da informação relativa ao campo de batalha a todos os níveis e a redução dos tempos de reacção, os comandantes dos escalões intermédios terão de tomar decisões baseados no conhecimento da intenção do comandante do escalão superior, sem muitas vezes ter tempo para consultas/planeamentos demorados.

Sem confiança na capacidade de decisão dos seus subordinados hierárquicos e uma efectiva descentralização, não será possível rentabilizar as oportunidades oferecidas por este novo conceito, já que as janelas de oportunidade têm que ser aproveitadas independentemente do nível e/ou escalão em que surgirem. A solução passa assim por apostar na descentralização do comando, com a concomitante desconcentração de meios, e na criação de uma cultura de aceitação do risco de decisões menos correctas, ou seja de aceitar partilhar o poder com as periferias do sistema. Obriga por sua vez a que todos os escalões tenham consciência perfeita da intenção do comandante.

Mas esta descentralização de modo algum é sinónima de desresponsabilização. Segundo Alberts&Hayes, está-se perante um novo conceito de liderança, que abandona o paradigma do Comando como “arte”, associada à pessoa do comandante, e do Controlo como “ciência” do Estado Maior, para assumir que comando e controlo são responsabilidade de todos.

A simples existência de uma info-estrutura é desafio suficiente para potenciais adversários tentarem a sua destruição ou disrupção, pelo que se torna necessário estar preparado para o “day after”. Daí que nas organizações centradas em rede, Comando e Controlo sejam intrínsecos ao funcionamento da organização e responsabilidade de todos os elementos. Aos comandantes da era da informação compete criar as condições iniciais (definir a missão, atribuir os meios, escolher as pessoas) para assegurar a geração dos comportamentos adequados que levarão todos os elementos da organização a agir e a tomar, em cada momento, as decisões certas, conformes com a missão e intenção inicialmente definidas. Mesmo no caso limite do desaparecimento, por uma qualquer razão, da info-estrutura.

Quanto à responsabilidade, esta será atribuída a cada elemento pela forma como se inseriu e como cumpriu a sua quota parte do plano inicial, bem como pelo modo como geriu os recursos



postos à sua disposição (Alberts et al., 2003, 201-211).

Assim, para se transformar o Exército numa estrutura da era da informação, não chega investir na tecnologia, é preciso alterar as atitudes face à disseminação da informação e às formas de executar tarefas e de atingir os objectivos. É crucial que a formação dos líderes militares seja reformulada<sup>20</sup>, em termos de capacidade de análise e gestão da informação que lhes é disponibilizada, de introdução de uma maior apetência pelo risco calculado, inerente à decisão, e da capacidade de **decidir em função do seu conhecimento da situação e do conhecimento da intenção do comandante**, de modo a combinar e tirar partido dos elementos do Potencial de Combate de forma mais eficaz (Fig. 17).

Esta pode ser a maior dificuldade pela necessidade de erradicar uma componente muito consolidada da cultura militar - a aversão pelo risco. Que será tanto maior quanto se considerar o potencial impacto político da acção a tomar, face á letalidade dos armamentos disponíveis e à coexistência no espaço de batalha, para além das populações, de outros jogadores, como as OI e ONG, sobretudo se se considerar a possibilidade de os resultados serem diferentes dos pretendidos.

À medida que a tecnologia muda, valores como a coragem, o enfrentar o inimigo cara-a-cara, perdem relevância e cresce a importância da competência técnica e da proficiência nos sistemas e tecnologias de informação e comunicações. No espaço de batalha do século XXI, o militar gestor é já o sucessor do militar herói.

#### 4.3.5 Interoperabilidade

Sendo a informação um recurso essencial ao funcionamento de qualquer organização, é a sua qualidade que constitui o factor multiplicador do potencial que faz a diferença, a força ou a fraqueza da organização. Enquanto recurso obtido em grande parte a partir do exterior das organizações, estas são forçadas a estabelecer interfaces com uma miríade de outras entidades, cada uma com o seu sistema de informação privativo. Neste enquadramento, a interoperabilidade é um factor crítico de sucesso.

Para a NATO, interoperabilidade é a “*capacidade dos sistemas, unidades ou forças fornecerem serviços e aceitarem serviços de outros sistemas, unidades, ou forças e utilizarem os serviços assim trocados, operando eficazmente em conjunto*” (NATO AAP-06). Trata-se de um conceito abrangente, em que a Interoperabilidade é vista nos aspectos técnico, operacional e de procedimentos.

---

<sup>20</sup> Bem como os sistemas de avaliação de desempenho e de avaliação de mérito.

Esta necessidade coloca-nos, no caso dos SI, perante a necessidade de garantir não só a interoperabilidade dos sistemas como principalmente a dos dados, suporte base de toda a informação.

Para responder a esta preocupação a NATO criou o conceito TIDE (**T**ransforming technology towards **I**nformation superiority, **D**ecision superiority and **E**xecution superiority). A partir da constatação da existência de um universo heterogéneo de múltiplas infra-estruturas, domínios, doutrinas, procedimentos e culturas no mundo dos SI, procurou-se definir uma metodologia e uma arquitectura comuns numa perspectiva integrada, de modo a criar um mesmo ambiente, onde o utilizador possa ir buscar a informação que precisa (Fig. 18).

Até muito recentemente, a integração dos sistemas existentes era feita ao nível vertical, de acordo com o modelo OSI<sup>21</sup>, à custa do desenvolvimento de interfaces físicos/lógicos entre sistemas, nunca garantindo uma interoperabilidade perfeita. O conceito TIDE aponta para a integração no nível horizontal, assente em serviços “Web” e alimentado ao nível do utilizador (Fig.19). Com serviços “Web” e uma arquitectura base comum, os SI em desenvolvimento poderão evoluir, incorporar novas funcionalidades, permitindo uma interoperabilidade plena, com redução dos custos associados ao desenvolvimento de interfaces para continuar a aproveitar os sistemas existentes (legacy systems).

#### **4.4 O Modelo Americano**

A implementação do conceito no Exército americano provocou a sua transformação numa força conjunta e expedicionária. A Transformação está a ser feita “top-down” com o objectivo de mudar a mentalidade das lideranças militares, de modo a garantir que as forças armadas serão capazes de conquistar e manter o domínio sobre o espaço de batalha, o tempo que for necessário, num cenário onde a regra é a incerteza.

O Army Campaigning Plan (Army Transformation Roadmap, 2004, 6-1 a 6-5) marca o ritmo da transformação. A chave está na mudança de todas as Brigadas da Active Component (AC) e respectivos Quartéis-Generais para estruturas modulares. Até 2020 a estrutura de comando de Divisões, Corpo e EAC (escalão acima do Corpo) irá ser substituída por 2 escalões de comando designados por UEx (com controlo táctico e operacional das Unidades combatentes) e UEy, que fornece as necessárias capacidades ao comandante das forças conjuntas (AnexoD).

A demonstração prática do conceito da força centrada em rede é a Brigada Stryker<sup>22</sup>, que

---

<sup>21</sup> OSI : Open Systems Interconnection é o modelo que define a estrutura das ligações em rede, um protocolo de interoperabilidade em sete camadas. O controle é passado de uma camada à seguinte, começando na camada física, relativa às ligações físicas até à camada mais alta, a das aplicações.

<sup>22</sup> Do nome da viatura que a equipa.

teve um papel fundamental para o sucesso da operação “Iraqi Freedom” pelas suas capacidades em TIC e pelas capacidades de sobrevivência.

#### 4.5 O Modelo NATO

Para a NATO, a decisão de mudar materializou-se na cimeira de Praga, através da criação do Comando Aliado da Transformação (ACT) em Norfolk e do levantamento de uma força, conjunta, a NATO Response Force (NRF), **tecnologicamente avançada**.

Na NRF confluem a vontade americana de transformar as forças europeias em forças convencionais capazes do uso intensivo da tecnologia, com a intenção da NATO de adquirir capacidades suplementares, moldadas à imagem das capacidades americanas.

Como o índice de rotação acordado para as participações nacionais é muito elevado (6 meses) esta força actua como catalizador da transformação das respectivas instituições militares nacionais, levando para os países de origem os conhecimentos e experiência adquiridos.

Ao mesmo tempo, serve para promover políticas coerentes de reequipamento/aquisição de equipamentos, o que, espera-se, virá a proporcionar a desejada interoperabilidade entre parceiros. Este desiderato foi reforçado na cimeira de Istambul<sup>23</sup>, tendo os ministros da defesa da NATO decidido aumentar para 40% o efectivo das forças nacionais que deverão ser estruturadas, preparadas e equipadas para operações no quadro da NATO e/ou de outras instâncias.

Por sua vez, em Jun2005, o NATO<sup>24</sup> Command Control and Consultation Board (NC3B) estabeleceu como princípios orientadores para os países membros da Aliança:

- Que se proceda à implementação assim que possível dos princípios do conceito NNEC e dos serviços associados;
- Que se estabeleça uma infraestrutura de “rede de redes” entre as diferentes Nações e entre as Nações e a NATO para suportar a experimentação, teste e validação dos conceitos NNEC;
- Que as capacidades, multi-nacionais e da NATO, de teste de Sistemas de Comunicações e Informações, tais como os CWID e CE<sup>25</sup>, sejam usadas para apoiar o planeamento operacional da NRF e para se alcançar a interoperabilidade entre os sistemas CIS das nações contribuintes;
- Que no processo de certificação das NRF seja avaliado o grau de interoperabilidade dos Sistemas de Comunicações e Informações (CIS);

---

<sup>23</sup> Junho de 2004.

<sup>24</sup> EAPC(AC/322)D(2005)0041 de 7Jun05, do Euro-Atlantic Partnership Council.

<sup>25</sup> Coalition Warrior Interoperability Demonstration (CWID) e o COMBINED ENDEAVOUR.

Para atingir este estágio de “Network Enabled Capability” a NRF terá de possuir aptidão para localizar e comunicar com todas as forças amigas bem como ser capaz de identificar as movimentações das forças inimigas, e ainda:

- Possuir aptidão para disponibilizar essa informação numa COP;
- Dispor de comunicações por satélite e de UAVs, especialmente para operações em áreas urbanas<sup>26</sup>;
- Dispor de meios ISR para aquisição atempada de informação relevante sobre as forças inimigas;
- Ter capacidade para despender os recursos financeiros imprescindíveis ao apetrechamento da força.

### **Síntese Conclusiva**

A informação é essencial para a tomada de decisões, para a compreensão do ambiente externo, a partilha da mesma visão da realidade e para adaptar a organização atempadamente. Estando a transformação do Exército a ser efectuada com recurso assumido às TIC, é imprescindível possuir-se capacidades de ponta nesta área. Como refere o General Loureiro dos Santos (2005, 1007), *“um país que reste marginal a este tipo de actividades científicas e tecnológicas não passará de um país falhado em relação às exigências da época em que vive e do ambiente que o envolve. Arrisca-se a ter uma capacidade muito limitada de agir na esfera internacional e dependerá de outros que se distanciaram nestas matérias”*.

Assim, e para “não perder a carruagem”, o Exército deverá dar passos concretos para:

- criar e estabilizar uma info-estrutura com a consequente criação de unidades vocacionadas para a recolha e tratamento da informação (ISTAR);
- transformar as suas forças em unidades modulares, com capacidade de projecção;
- proceder ao reajustamento cultural dos seus militares, no sentido de as futuras forças estarem aptas a actuar em moldes conjuntos;
- assegurar a existência de sistemas de comunicações e de informação interoperáveis com os dos outros Ramos e os tradicionais parceiros da cena internacional;
- estreitar a cooperação com a indústria nacional, ajustando os processos de aquisição no sentido de os novos materiais virem já dotados da capacidade de interligação em rede.

---

<sup>26</sup> Por incapacidade das redes tácticas satisfazerem os requisitos de comunicações, em termos de Largura de Banda e de segurança.

## Capítulo 5 - AS TIC NO EXÉRCITO PORTUGUÊS

*As organizações mais competitivas são as que melhor gerem os seus SI  
Michael Porter*

### 5.1 Enquadramento e Orientação Política

Segundo o preconizado no Livro Branco da Defesa (2001), é indispensável “*evoluir para uma **arquitectura de comando e controlo nacional conjunto** e para ... se dispor de uma adequada **capacidade conjunta** de recolha e processamento de informações militares, assente em meios de vigilância, reconhecimento e detecção.*”

Este propósito, vertido no CEM (2003)<sup>27</sup>, foi reiterado pelo MDN<sup>28</sup> ao considerar ser “*uma clara prioridade no processo de reestruturação e de modernização das Forças Armadas, a **construção de uma efectiva capacidade de acção conjunta...** tornando as Forças Armadas aptas a actuar de forma mais integrada e em estreita cooperação com outras forças aliadas*”.

Estas tomadas de posição, que indicam uma clara opção por um modelo de forças conjuntas, são complementadas com o compromisso assumido por Portugal relativamente à implementação do conceito NNEC, em que o EMGFA, em resposta ao ACT, assumiu em 2005 como ambição nacional, a concretizar num espaço de 10 a 15 anos ([www.nnec.act.nato.int](http://www.nnec.act.nato.int)):

- *To establish a national NEC vision and provide a network centric approach supporting forces re-structure and management from strategic to tactical level;*
- *To develop a strategic concept as a sound basis for increasing of operational readiness, interoperability, mobility, modularity and versatility;*
- *To involve the national research and defense industry cluster in the process of developing the required capabilities, either domestically or in cooperation with the allies.*

### 5.2 Planeamento de Médio e Longo Prazo. Plano Director de Sistemas de Informação

O modelo OD, modelo de mudança das organizações, preconiza como um dos passos dum qualquer processo de transformação, o desenvolvimento de uma “visão” para a mudança e de se “ganhar o comprometimento para a visão” (Magalhães, 1999, 29).

No caso do Exército, a “VISÃO” para esta área consta de directivas e despachos avulsos, tendo a sua concretização sido remetida, por norma, para a LPM. Apesar de tentativas várias, desde o início da década de 90, nunca foi elaborado um **plano director** que estabelecesse uma **Visão** do Exército para os Sistemas de Informação e Comunicações. Um plano que definisse as

---

<sup>27</sup> Que estabelece a ideia de centralização de valências, passando pela utilização conjunta de instalações ou mesmo, sempre que possível, o funcionamento integrado dos Ramos das FA.

<sup>28</sup> Discurso no dia das Forças Armadas, em Estremoz, em 25 de Junho de 2005.

orientações gerais e objectivos específicos, traduzível num plano de aquisições e reequipamento, e levasse à consequente reorganização da estrutura de apoio (Unidades) e de recrutamento do pessoal para implementar, manter e “alimentar” essa estrutura.

Este instrumento, indispensável para uma gestão racional de recursos humanos e logísticos, começou agora a tomar forma, através da publicação do **Plano de Médio e Longo Prazo** (PMLP) do Exército (Agosto de 2005), que estabelece metas e os objectivos a concretizar até 2023. Em simultâneo, está a ser preparado no MDN o **Plano Director de Sistemas** para a Defesa<sup>29</sup> o qual poderá servir de base para a elaboração de um documento congénere para o Exército,<sup>30</sup> que sirva de elemento congregador de vontades e forneça a moldura enquadadora do emprego das TIC que tem faltado.

### 5.3 Sistema C4I

No âmbito da info-estrutura das forças armadas, pode considerar-se existir já a base de um sistema integrável, de comunicações e sistemas de informação, que disponibiliza um conjunto significativo de serviços e funcionalidades (faltando apenas a vontade das partes para o mesmo passar a integrado), e que a seguir se elencam:

#### 5.3.1 Estrutura de Comunicações

- SICOM<sup>31</sup> : rede de comunicações militares que integra as redes privativas dos Ramos e garante a interligação com a NATO;
- IESFA : rede de comunicações segura, classificada NATO SECRET, System High e com um interface (IEG),<sup>32</sup> com a NATO SECRET WAN;
- INTRANET Segura da Defesa, assente no SICOM e nas redes privativas dos Ramos;
- Interface BLOS<sup>33</sup> em HF e SATCOM com as forças móveis e/ou destacadas do SFN;

Para além dos sistemas refenciados, há ainda a considerar os respectivos serviços de Gestão centralizada de Directorias Telefónicas e de Gestão de Segurança.

#### 5.3.2 Estrutura de Informação

A estrutura de informação das Forças Armadas é composta por sistemas proprietários, dos Ramos e da NATO, que contribuem para a construção da imagem operacional comum (COP) bem como para acesso a áreas funcionais específicas da NATO (FASS<sup>34</sup>).

Num futuro próximo deverá fazer ainda parte desta estrutura o novo sistema integrado

---

<sup>29</sup> Despacho 236/MDN/2005, de 20 de Outubro de 2005.

<sup>30</sup> Plano Director SIC, que estabeleça uma política geral para as TIC, através da definição de Standards e Arquitectura Comum, para a constituição de uma Infra-estrutura de Informação da Defesa e Forças Armadas.

<sup>31</sup> SICOM: Sistema Integrado de Comunicações Militares.

<sup>32</sup> Information Exchange Gateway.

<sup>33</sup> Beyond Line of Sight.

<sup>34</sup> FASS : Functional Area Sub System.

de gestão (SIG), que irá disponibilizar serviços comuns nas áreas Financeira e de Gestão de Recursos (Humanos e Materiais).

#### **5.3.2.1 COP-Common Operational Picture**

É o resultado das diferentes “imagens” disponibilizadas pelos sistemas de comando e controlo dos Ramos, a saber :

- MCCIS, sistema de comando e controlo naval;
- ICC, sistema de comando e controlo da Força Aérea;
- SICCE/JOIIS, sistema de comando e controlo terrestre.

#### **5.3.2.2 FASS**

- LOGFAS, sistema logístico da NATO;
- BICES/LOCE, sistema de informações multinacional (BICES) e americano (LOCE).

#### **5.3.2.3 Sistema de Informação de Gestão (SIG)**

- SAP R3, o futuro Sistema Integrado de Gestão (SIG), em desenvolvimento.

#### **5.3.3 Serviços Comuns**

- Serviço de Tráfego registado (mensagens) ACP 127 e MMHS;
- Serviço de Voz – rede telefónica privada das Forças Armadas;
- Serviços de Web Browsing, de e-mail, video conferência e imagem seguros, apoiados na rede IESFA (System High).

### **5.4 Info-estrutura do Exército**

A info-estrutura operacional do Exército assenta no sistema SIC-T, projecto em desenvolvimento na EMEL, formado por uma componente de comunicações, o SITACO, e uma de informação, o SICCE.

Estas duas componentes, cujo desenvolvimento se vem arrastando durante anos, receberam um impulso decisivo em 2002 com a criação de um GT na dependência do general VCEME, e coordenado pelo MGen DST, para estudar e propor uma arquitectura técnica e funcional para o sistema<sup>35</sup>. Esta arquitectura, aprovada em Janeiro de 2004, encontra-se em fase de implementação (Anexo E).

#### **5.4.1 Comunicações tácticas. O SITACO**

O SITACO, sistema de comunicações táctico baseado no rádio PRC 525 (com tecnologia M3TR<sup>36</sup>), deverá fornecer comunicações seguras, de voz, dados (imagem fixa e video) e mensagens, estando em estudo o seu upgrade para disponibilizar serviços Web (Internet Táctica) aos escalões Batalhão e Companhia.

---

<sup>35</sup> Despacho 29/VCEME/2002.

<sup>36</sup> MT3R: Multirole, Multiband, Multifunction Transmition Radio.

O rádio 525 embora não seja ainda um Software Defined Radio-(SDR), permitirá a realização de operações conjuntas e combinadas, graças à sua facilidade de integração com sistemas antigos (legacy systems) ainda em uso, ao mesmo tempo que responde às exigências que os actuais sistemas apresentam. A flexibilidade que oferece, por ser um rádio com algumas parametrizações por software, permite que se integre em redes tácticas como um elemento da CNR (Combat Network Radio), ao mesmo tempo que serve de interface para sistemas fixos como as redes digitais ISDN, e funciona ainda como um vulgar terminal telefónico.

Ao nível das comunicações estratégicas/operacionais, está no entanto a recorrer-se cada vez mais a comunicações por satélite, realidade incontornável face aos volumes elevados de informação criados pelo conceito de guerra centrada em rede, o que representa um sério desafio para os países que, como Portugal os não possuam, dependentes que ficam do apoio prestado pela NATO.

Se este aspecto não for considerado, e vingar a tese defendida por alguns países de *“quem não tiver comunicações, não precisa de se incomodar em aparecer”*, Portugal poderá ver coarctada a sua participação nas intervenções aliadas e por esta via, ver seriamente afectado o seu peso na cena internacional.

#### **5.4.2 Sistema de Informação para Comando e Controlo do Exército - SICCE;**

Tendo tido a sua origem na evolução de um programa de simulação, o VIGRESTE, o SICCE, é um projecto de I&D, formalmente iniciado em 1998, e ainda na **fase de protótipo**. O SICCE constitui a estrutura base de informação táctica do Sistema de Forças do Exército Português, visando ser utilizado na actividade regular de Estado Maior dos Comandos e Quartéis Gerais de GU. Este sistema, já instalado no COFT, nas GU e nas FND, fornece ao utilizador as seguintes funcionalidades:

- Situação Operacional Comum (COP);
- Informação geográfica (GIS) com ficheiros raster e vectoriais;
- Visualização do terreno a duas e três dimensões;
- Transparentes de Operações, Planos e Ordens;
- Cálculo dos Potenciais de Combate e Gestão de Ordens de Batalha.

No esforço de garantir a interoperabilidade do sistema com os congéneres europeus e da NATO, a equipa de desenvolvimento integra desde o início do projecto vários grupos NATO e multinacionais. Destes, o mais importante é o MIP, (Multilateral Interoperability Program) criado em Abril de 1998 no Canadá, com a participação da França, Alemanha, Itália, Inglaterra e EUA . Este grupo tem como objectivo alcançar a interoperabilidade internacional em sistemas de comando e controlo, do escalão CE ao batalhão e inferiores.



### 5.4.3 Sistema de Informação de Gestão (MIS)

Encontra-se, desde 2002, em implementação na área da defesa um sistema de informação de gestão único, o Sistema Integrado de Gestão (SIG) que integra as diferentes funções administrativo-logísticas<sup>37</sup>.

O SIG baseia-se numa aplicação comercial, o SAP R-3, e assenta no conceito de uma Base de Dados única, onde os dados são introduzidos apenas uma vez, ficando imediatamente disponíveis às diferentes áreas funcionais (financeira, logística e de recursos humanos) .

O processo de implementação deste sistema não foi coordenado com o processo de desenvolvimento do SICCE, não havendo de momento interoperabilidade entre sistemas, pelo que há a necessidade de se estabelecerem interfaces entre estes, de modo a garantir que a informação comum possa fluir entre os sistemas.

Por sua vez, a extensão às UEO deste sistema vai colocar uma pressão acrescida sobre os actuais sistemas de comunicações, em termos de segurança, fiabilidade e resiliência, que levou já à manifestação da intenção, por parte do MDN, de criar um órgão (Agência/Instituto) que centralize a gestão da rede de comunicações SICOM<sup>38</sup> e crie uma infra-estrutura comum de comunicações da Defesa.

## 5.5 O Modo Conjunto

Considerando-se ser a actuação em conjunto um estado de espírito, assente no ensino, tradição e no hábito, a realização de exercícios conjuntos é um passo determinante para a criação e manutenção dessa mentalidade.

Através das séries de exercícios LUSÍADA, EOLO, SWORDFISH e outros, o Exército tem vindo a pôr em prática este conceito. No entanto, a sua rentabilização pode ser maximizada se for coordenada com o ciclo bienal do planeamento de forças, de modo a:

- Usar os exercícios para validar novos conceitos doutrinários;
- Usar a experiência para recolher “lessons learned” com implicações na doutrina, organização e equipamento;
- Incorporar as alterações resultantes das “lições aprendidas” no ciclo seguinte.

Outro dos passos para a criação de uma mentalidade conjunta, é o desenvolvimento de hábitos de partilha de informação. Este desiderato pode ser atingido com a activação de uma rede de informação comum, a Intranet da defesa. Em 2001 foi identificada esta necessidade, bem como a possibilidade de concretização no curto prazo, mas incompreensivelmente a Intranet Segura da defesa é, ainda, apenas uma realidade potencial.

---

<sup>37</sup> Despacho orientador 109/MEDN/02,

<sup>38</sup> SICOM : Sistema Integrado de Comunicações Militares

O conceito desta rede assenta na interligação das Intranets de cada Ramo<sup>39</sup>, com mecanismos de segurança adequados, de forma a constituir repositório comum de informação que espelhe o que cada uma das entidades intervenientes pretender divulgar (Fig. 20).

O acesso a esse repositório comum de informação deverá ser feito através de um “Portal” da Defesa, que será o integrador de todos os serviços e o ponto de acesso do militar à Instituição. Ao ligar-se à rede, cada militar terá acesso ao seu ambiente de trabalho, com o respectivo perfil de acessos que lhe permita executar as tarefas inerentes à sua função. Atendendo à sua universalidade, a Intranet deverá constituir-se também no elo de ligação entre o Território Nacional e as Forças Nacionais Destacadas.

## 5.6 Simulação

*“Um dos factores que complica a transformação é a necessidade de demonstrar a eficácia operacional potencial de um conceito novo. A capacidade de experimentação e de simulação, na sua componente de jogos de guerra foi, no passado, crítica para os líderes visionários acelerarem a aprendizagem e conseguirem reunir as provas necessárias para justificar os investimentos nas novas capacidades”* (Garstka, 2005, 9-10).

Em sintonia com este conceito, o PMLP do Exército aponta para a “necessidade de potenciar e incentivar a utilização do Sistema de Simulação CAX, permitindo a realização de exercícios com intervenção da EBE, de forma a melhorar e tornar mais eficaz o treino e aprontamento das forças”.

O Exército dispõe já de um sistema de simulação e apoio à decisão, o SIMOPMIL, originalmente “VIGRESTE”, instalado no ex-IAEM. Este sistema nasceu formalmente em 1989, a partir de um projecto de I&D da EPT. Apesar de, na sua génese, contemplar o apoio ao planeamento e acções de EM, nos escalões Batalhão e Brigada, foi a faceta de jogos de guerra que recebeu o impulso decisivo.

O sistema foi desenvolvido pela mesma equipa que criou o SICCE e, por falta de massa crítica em recursos humanos, encontra-se desactualizado e não está devidamente documentado. Deste modo, a sua industrialização e exploração sustentada passa pelo “reverse engineering” se se recorrer a empresas exteriores ao Exército, ou pelo hipotecar a tempo inteiro da equipa de desenvolvimento, ainda que com eventual prejuízo das actividades que decorrem no fórum do Comando e Controlo (SICCE).

Esta situação é o reflexo de não ter existido, na área de simulação, uma política clara do Exército, orientada para a definição de objectivos palpáveis e de uma estrutura organizacional

---

<sup>39</sup> Despacho n.º 72/MDN/2001 - Constituir uma Intranet segura da Defesa;

sustentável. A ultrapassagem desta situação passa pela adesão aos programas de simulação da Aliança (Path Finder e DiMuNDS2000) e pela adopção da arquitectura adoptada pela NATO (HLA:High Level Architecture) de modo a possibilitar a sua integração na rede de sistemas dos parceiros aliados.

Existindo um sistema C2, o futuro sistema de simulação deverá ser integrável com o mesmo, de modo a criar e rentabilizar sinergias entre os dois sistemas, aproveitando a sua co-localização.

### **5.7 Interoperabilidade**

O reconhecimento da necessidade de interoperabilidade entre sistemas de comunicações e de informação deu origem, na NATO, a dois programas de exercícios, onde são testados sistemas e equipamentos: o CWID (NATO) e COMBINED ENDEAVOUR<sup>40</sup>. Nestes exercícios, as nações são incentivadas a participar com os respectivos sistemas de comando e controlo para testar a interoperabilidade com os sistemas NATO (MCCIS<sup>41</sup>, JOIIS<sup>42</sup> e ICC<sup>43</sup>). A finalidade destes “fora” é a de encontrar soluções para a integração de plataformas aplicacionais heterogéneas, num ambiente “Web”. Dirigem-se às áreas de correio electrónico, troca de mensagens formatadas<sup>44</sup>, processamento e disseminação de informação bem como aos mecanismos de replicação de dados.

Já o COMBINED ENDEAVOUR é um forum mais alargado que procura testar a interoperabilidade não só entre SI mas também entre sistemas de comunicações, estando por isso indicado para a avaliação das capacidades do novo rádio que irá equipar o Exército, o PRC 525.

Actualmente o Exército participa no Combined Endeavour com o SICCE, com sucesso unanimemente reconhecido, mas para garantir a interoperabilidade entre meios de comunicação importa também introduzir o PRC 525 neste forum.

Ainda no que se refere ao PRC 525, e no âmbito da implementação da “NATO Network Enabled Capability”, existe um grupo criado pela NATO para estabelecer as bases de uma nova tecnologia que irá possibilitar maior largura de banda para os rádios de combate, e para garantir a interoperabilidade entre parceiros da Aliança, o “Software Defined Radio (SDR) Internacional Forum”, grupo que se considera que o Exército deveria integrar.

---

<sup>40</sup> Patrocinado pelos EUA, com a participação dos restantes países NATO e PfP.

<sup>41</sup> MCCIS: Maritime Command and Control Information System é o sistema de C2 usado pelas Marinhas NATO. Recebe e envia dados para os sistemas JOIIS e ICC

<sup>42</sup> JOIIS : Joint OPS/INTEL Information System, é um sistema usado pela NATO para obter a COP através da Recognized Ground Picture. Recebe e envia dados para os sistemas MCCIS e ICC.

<sup>43</sup> ICC : Integrated Air Command and Control for Air Operations, antes Interim CAOC's Capability, é um sistema usado nos CAOC NATO e adoptado por alguns países, entre os quais Portugal, como o seu sistema de C2 aéreo. Recebe e envia dados para os sistemas MCCIS e JOIIS.

<sup>44</sup> Mensagens AdatP-3 e OTH Gold.

## 5.8 Indústria Nacional

O Programa do XVII Governo, preconiza o “*desenvolvimento do Sector Empresarial na Área da Defesa, e a integração das indústrias de defesa portuguesas nas redes europeias de criação de valor de indústrias de defesa, com vista ao estabelecimento de uma base tecnológica e industrial de Defesa e um mercado de equipamentos de defesa*”. Nesta linha, os desenvolvimentos em curso no Exército têm sido feitos com base nas empresas EID e EDISOFT, membros da EMPORDEF.

Contudo, as lições do passado apontam para que os projectos que não são objecto de um acompanhamento rigoroso por parte do Exército, acabam por sofrer sérios desvios em termos de cumprimento de requisitos, de prazos e de orçamentos. Apesar da competência técnica que lhe é geralmente reconhecida, as dificuldades manifestadas prendem-se com a “insuficiência de recursos humanos e nalguns casos com a falta de capacidade financeira para o desenvolvimento e execução dos projectos”<sup>45</sup> por parte das empresas desta área.

A criação das Missões de Acompanhamento e Fiscalização (MAF) forneceu um mecanismo precioso para executar o objectivo enunciado no programa do governo, de colaboração entre Indústria Nacional e Forças Armadas, sem com isso sacrificar a operacionalidade da força. Tendo sido considerados como determinantes no processo de transformação do Exército, os programas de:

- aquisição de Viaturas Blindadas de Rodas;
- aquisição de Helicópteros Ligeiros e Helicópteros Médios;
- substituição de CC M60 e a modernização das viaturas da família M113;

dever-se-á, durante os processos de aquisição, garantir o acompanhamento destes programas, com a preocupação de assegurar a interoperabilidade dos respectivos sistemas de comunicações, com as especificações do SITACO, com os meios dos outros Ramos e os dos nossos parceiros, bem como a capacidade de operar em rede.

Para colmatar as insuficiências de recursos humanos acima mencionadas, deveria ser ponderado o envolvimento de militares, técnicos e operacionais, no desenvolvimento dos projectos.

## 5.9 Organização

Na área CIS tem-se verificado um défice organizacional crónico, sem que exista uma linha clara de orientação relativa às políticas de comunicações e dos sistemas de informação, nas suas duas vertentes, a de gestão (MIS) e a de Comando e Controlo.

---

<sup>45</sup> Relatório da Assessoria Técnica do Conselho de Comunicações da Defesa, Maio de 1999.

Com a reorganização de 1993 (DecLei 50/93 de 26Fev) a situação agravou-se, por força da colocação da Direcção dos Serviços de Transmissões no canal logístico, na dependência do TGen QMG. A gestão e desenvolvimento dos sistemas de informação de gestão ficou no CIE, dependente do TGen VCEME (após uma efémera passagem pela DST) e a dos sistemas de informação de comando e controlo entregue à EPT. Vive-se assim uma situação peculiar, em que ao Director da DST, com competências exclusivamente logísticas, são exigidas respostas a problemas e situações de cariz operacional, sem que este tenha competência sobre as unidades executoras.

Em 2000, numa tentativa de racionalização e de reconhecimento da importância das TIC, bem como de dotar o EME de meios para realizar o planeamento de médio e longo prazo, foi ali criada uma Divisão de Comunicações e Sistemas de Informação (DCSI), mas que só esporadicamente tem sido enquadrada e guarnecida com o pessoal necessário.

As resistências internas levantadas ao modelo organizacional implementado conduziram à elaboração de um estudo, feito pelo EME e DST, que apontou para a criação, na estrutura superior do Exército, de uma Direcção de Comunicações e Sistemas de Informação, resultante da fusão da DST, da DCSI/EME e dos vários órgãos CIS existentes (RT e CIE). Esta Direcção, vocacionada para “maximizar a utilização de tecnologias de informação, instrumento indispensável para potenciar as capacidades operacionais”<sup>46</sup>, teria a responsabilidade de:

- promover a orientação estratégica e as definições políticas dos sistemas de comunicações e dos sistemas de informação;
- coordenar actividades relacionadas com a gestão de informação do Exército, tais como a administração de dados;
- coordenar o apoio ao utilizador dos sistemas de comunicações e sistemas de informação do Exército.

A estrutura e dependência desta Direcção, inicialmente na dependência do TGen VCEME, foi reformulada ainda antes de ser implementada, tendo sido colocada na estrutura do COFT o que se afigura uma decisão redutora da sua importância, uma vez que a esfera de acção da Direcção é transversal a todo o Exército e abarca todos os SI, sejam operacionais ou de gestão.

Esta postura contrasta com a importância que o MDN atribuiu às TIC, traduzida no desencadear de um processo de criação de agências/institutos que irão centralizar o planeamento, desenvolvimento e gestão dos SI e das Comunicações na área da defesa. Com esta decisão e com a incorporação do remanescente do Centro de Informática do Exército no Regimento de

---

<sup>46</sup> Directiva N.º 263/CEME/01 de 19Dez01

Transmissões, o Exército está-se a auto-limitar à condição de mero implementador de sistemas e de prestador de serviços de “help desk”.

Já no que diz respeito às Companhias de Transmissões das Brigadas e das Forças de Apoio Geral, a sua reorganização está a ser efectuada com base na arquitectura resultante do programa SIC-T, estando à partida criadas condições para que esta componente da info-estrutura venha a ser coerente com o conceito NCW na linha do definido pelo CEDN :

- dotar o Exército com facilidades de comunicações e SI, interoperáveis e com capacidade de interacção em rede;
- assegurar a ligação entre redes CIS do Exército e as estruturas nacionais congéneres bem como com as das organizações de segurança e defesa que Portugal integra.

O mesmo se passa com o levantamento previsto de uma capacidade ISTAR na Brigada de Intervenção, a concretizar até final de 2010 e, por outro lado, através de um sistema ISTAR no Force Goal EL 583 Division/Brigade Level, este sem data especificada.

#### **5.10 Mudança de Mentalidades**

A limitada “cultura tecnológica” da maioria dos quadros superiores do Exército tem como consequência a dificuldade em perceberem quais as reais vantagens das utilizações das TIC do que decorre a tentação para isolar os problemas das TIC em torno dos “especialistas”.

Para ultrapassar esta situação há necessidade de incentivar a formação tecnológica dos quadros do Exército, por forma que, a prazo, seja possível obviar esta deficiência de base. E isso porque, mesmo para uma mudança suave e pacífica é imperativo mobilizar vontades e disponibilidades, como definido pelo modelo OD. Sendo a introdução do conceito de guerra centrada em rede, uma mudança revolucionária pelas implicações que acarreta, esta necessidade tem maior acuidade e é necessário criar mecanismos para sensibilização e conseguir a adesão de todos os quadros a esta mudança.

Na formação ministrada na Academia Militar, de cariz essencialmente social após a reforma escolar de 2000, os cursos das Armas passaram a assentar nas áreas de sociologia, gestão e estudos internacionais, desvalorizando o estudo das ciências exactas (física e matemática) bem como o estudo das tecnologias de informação e comunicações.

Tendo sido reconhecido que esta preparação não proporciona aos futuros oficiais as ferramentas indispensáveis a um exercício adequado da sua função de líderes e gestores, está a ser preparada uma alteração curricular no sentido de reintroduzir matérias como a Física e as TIC, bem como de reforçar o ensino da matemática em todos os cursos, alterações a implementar em 2006/2007 (Directiva 244/CEME/2005).

Nas palavras do Comandante da AM, “*para além de no perfil do oficial do exército ter de*

*existir uma componente estritamente militar, o sentir militar, há que considerar que no cumprimento da missão, o oficial tem de gerir recursos humanos, materiais e financeiros, para que precisa de possuir uma mentalidade analítica, treinada para a tomada de decisões<sup>47</sup>”.*

Já na preparação dos futuros dirigentes, a fusão dos três Institutos Superiores no Instituto de Estudos Superiores Militares (IESM) e a integração num único curso, conjunto, dos diferentes cursos de promoção a oficial general, é um passo auspicioso para a formação de uma mentalidade conjunta, indispensável à introdução nas Forças Armadas do conceito de guerra centrada em rede. Falta realizar a junção, em Pedrouços, dos polos da Junqueira (Marinha) e de Sintra (Força Aérea) de modo a concluir-se o processo e a dar um sinal claro de que o conceito de “conjunto” não é, apenas, mais um vocábulo no léxico militar português do século XXI.

### **Síntese Conclusiva**

Numa perspectiva de implementação do conceito de guerra centrada em rede, pode concluir-se que nos últimos anos se têm vindo a dar passos importantes na direcção correcta, se bem que as actividades desenvolvidas careçam do adequado enquadramento conceptual.

Não existindo o documento que permita orientar e canalizar esforços de forma harmoniosa e concorrente, é previsível que se mantenha o tradicional défice organizacional nesta área (dificuldades na constituição do órgão gestor e da estrutura de apoio à EBE) bem como as já tradicionais dificuldades ao nível dos sistemas de comando e controlo e de simulação, que precisam de passar da fase de protótipo de sucesso, para a de produto acabado.

## **Capítulo 6 – CONCLUSÕES**

*O nosso ponto forte é a conceptualização, mas a concretização é o nosso ponto fraco*  
Carlos Zorrinho

A evolução das TIC provocou a compressão dos níveis da guerra, obrigando a “encarar” a sua influência numa perspectiva global, que afecta igualmente os níveis estratégico, operacional e tático.

A facilidade na aquisição, tratamento e disseminação da informação, introduziu, na condução das operações, a compressão do ciclo de tomada de decisão.

Estas alterações valorizaram o elemento humano, tendo dado origem a novos paradigmas de liderança, com ênfase para a descentralização da decisão e com o abandono progressivo do conceito do “herói-soldado” em favor do militar técnico, funcionalmente confortável com as novas tecnologias.

---

<sup>47</sup> Excerto de entrevista realizada no âmbito da pesquisa

Ao nível organizacional (físico) as forças passaram a organizar-se em unidades modulares, projectáveis, preparadas para actuar em conjunto.

Já ao nível da informação, as TIC criaram um mundo ligado em rede, assente em plataformas inteligentes, com preocupações acrescidas de interoperabilidade entre sistemas e maior exigência no relacionamento com as indústrias de defesa, numa perspectiva de comprar menos mas melhor.

No nível cognitivo, as novas tecnologias introduziram novos paradigmas da partilha da informação, dando origem ao aparecimento do “guerreiro do conhecimento” de Peter Drucker.

O estudo efectuado permite constatar que a Transformação em que o Exército está empenhado assenta na construção de uma estrutura operacional baseada em unidades modulares, apoiadas por unidades CIS levantadas em torno dos conceitos resultantes do programa SIC-T. Assim, e no que concerne à adesão a uma capacidade centrada em rede, pode concluir-se que se está na direcção correcta.

No entanto, ao longo do estudo foram identificadas áreas que se considera necessitarem de especial atenção e em relação às quais se sugere:

- Na área da gestão da informação, deverá ser criado um Plano Director de Sistemas, que faça a ligação entre a VISÃO aprovada pelo TGen VCME (mas não divulgada) e as medidas elencadas no Plano de Médio e Longo Prazo. Este Plano deverá ser o elemento agregador de vontades e do comprometimento dos quadros para a transformação em curso;
- Proceder-se o mais rapidamente possível ao levantamento da Direcção de Comunicações e Sistemas de Informação, o qual aguarda a concretização desde 2002, por forma a responder às necessidades de normalização dos modelos de dados dos SI (de Gestão e Comando e Controlo) do Exército, a garantir a interoperabilidade entre sistemas e a assegurar a sustentabilidade dos mesmos;
- Operacionalizar a Intranet de defesa de modo a criar hábitos de partilha da informação e como primeiro passo para a formação de uma infoestrutura, com base no IESFA;
- Ajustar a doutrina e procedimentos aos novos paradigmas de partilha de informação e de liderança decorrentes do conceito NCW e activar programas de formação e treino conjuntos;
- Rever os programas curriculares da Academia Militar no sentido de repôr o ênfase da formação dos futuros oficiais na formação em ciências exactas, com especial destaque para a proficiência nas TIC;
- Na área das aplicações, proceder à consolidação do SICCE e VIGRESTE, em termos



de produto acabado (documentação, registo de patente e expansão/comercialização dos sistemas), lançando as bases para uma utilização mais confiante e intensiva, bem como para a aquisição de uma efectiva capacidade de sustentação do sistema;

- Concorrentemente, proceder à integração das funcionalidades entre os dois sistemas (de simulação e de comando e controlo) explorando a criação e rentabilização de sinergias entre os dois sistemas;
- Estreitar o relacionamento com a indústria nacional, numa perspectiva de parceria versus financiamento, apostando na monitorização adequada dos projectos, através da prossecução da actividade de fiscalização e acompanhamento das MAF para os programas de vulto. Será desejável continuar a colaboração existente do passado mas sem sacrificar a operacionalidade das forças a eventuais aquisições de know-how e potenciais criações de nichos de competência de eficácia duvidosa para a economia nacional.

*“A única forma de descobrir os limites do possível é ultrapassá-los até ao impossível”*, diz a 3ª Lei de Clarke (Clarke, 2001, 12). As medidas aqui elencadas são os primeiros passos, incontornáveis, no longo caminho para a construção, pelo Exército, de uma capacidade centrada em rede.

A preocupação constante com a interoperabilidade dos sistemas (existentes e a implementar), e com a mudança de mentalidades, cultura e comportamentos são os grandes desafios a vencer, muito mais que a aquisição de soluções tecnologicamente sofisticadas.

Sobretudo porque, *“o desafio que se coloca aos instrumentos militares da actualidade é que não chega estar pronto para combater a próxima guerra, mas sim procurar em simultâneo, responder à Revolução dos Assuntos Militares e da Transformação e preparar-se para a guerra, que virá depois da próxima.”* (Ramalho, 2005, 772).

IESM, 13 de Março de 2006

Rui M. S. Rodrigues

CorTmEng

## BIBLIOGRAFIA

### Livros

ALBERTS, Dr. David S. “ *The Unintended Consequences of Information Age Technologies*”, National Defense University NDU Press Book, Abril 1996.

ALBERTS, David S. “*Information Age Transformation : Getting to a 21<sup>st</sup> Century Military*”, CCRP Publication Series, Março 2003.

ALBERTS, David S.; GARSTKA, John J.; HAYES, Richard E. “*Network Centric Warfare: Developing and Leveraging Information Superiority*”, CCRP Publication Series, 1999.

ALBERTS, David S.; GARSTKA, John J.; HAYES, Richard E.; SIGNORI, David T. “*Understanding Information Age Warfare*”, CCRP Publication Series, Outubro 2004.

ALBERTS, David S.; HAYES, Richard E. “*Power to the Edge*”, CCRP Publication Series, Junho 2003.

ALBERTS, David S.; GARSTKA, John J.; STEIN, Frederick P. “*Network Centre Warfare*”, CCRP Publication Series, Outubro 2003.

ALVES, General José Lopes. “*ESTRATÉGIA Panorama Geral da Sua Teoria*”, Publicações D. Quixote, Lisboa, Fev99.

BOUTHOU, Gaston. “*O Fenómeno Guerra*”, Estúdios Cor, Lisboa, 1966.

BORGES, João Vieira. “*Intervenções Militares Portuguesas na Europa do Séc. XVIII*”, Edições Atena, Sintra, 2000.

CLARKE, Arthur C. “*Visões do Futuro*”, Notícias Editorial, 2001.

CLAUSEWITZ, Carl von. “*Da Guerra*”. Perspectivas & Realidades, Lisboa, 1976.

COUTO, Cabral. “*Elementos de Estratégia*”. Lisboa, IAEM, 1998.

DINIS, José A. Henrique. “*Guerra de Informação*”, Edições Sílabo, Set 2005.

DOS SANTOS, General Loureiro. “*Apontamentos de História para Militares*”, IAEM, Lisboa 1979.

DOS SANTOS, General Loureiro. “*Incursões no Domínio da Estratégia*”, Fundação Calouste Gulbenkian, Lisboa, 1983.

GOMES, Carlos de Matos. “*MOÇAMBIQUE 1970. Operação Nó Górdio*”, Tribuna da História, Lisboa, 2002.

HOLDER, L. D. *"Operational Art in the US Army: A New Vigor, Essays on Strategy III"*; Washington, D.C., National Defense University Press, 1986.

JABLONSKY, David. *"Strategy and the Operational Level of War: Part I,"* Parameters Vol. XVII, No. 1, Spring 1987.

LEANDRO, TGen Garcia. Editorial da Nação e Defesa nº 107, IDN, 2004.

METZ, Steven; KIEVIT, James. *"The Revolution in Military Affairs and Conflict Short of War"*, CCRP Publication Series, June 1994.

METZ, Steven. *"Strategy and Revolution in Military Affairs: From theory to Policy"*, CCRP Publication Series, June 1995.

METZ, Steven. *"Armed Conflict in the 21<sup>st</sup> century: The Information Revolution and post-Modern Warfare"*, Strategic Studies Institute, Abril 2000.

NYE, Joseph S. Jr. *"Compreender os Conflitos Internacionais"*, Gradiva, Lisboa, Maio de 2002.

ROCHA, Álvaro. *"Maturidade da Função Sistemas de Informação: Teoria dos Estádios, Modelos e Avaliação"*, UFP, Março 2002.

RODRIGUES, Luís Silva. *"Arquitecturas dos Sistemas de Informação"*, Coleções FCA, Lisboa, Julho 2002.

SALAZAR, Maria da Saudade. *"As Forças Armadas Portuguesas - Desafios numa Sociedade em Mudança"*, Editora Caleidoscópio, Lisboa, 2005.

### **Artigos**

BISPO, António. *"As Operações Militares no Quadro das Novas Tecnologias. O Conceito de Network Centric Warfare"*. Revista Militar nº 10, Outubro 2004.

BOOT, Max. *"The New American Way of War"*, Foreign Affairs, vol. 82, nº4. July/August 2003.

CEBROWSKI, Arthur C.; GARSTKA John J. *"Network-Centric Warfare: Its Origin and Future"*, Proceedings Magazine, 1998.

FOROOHAR, Rana. *"Learning to Share"*. Newsweek Special Edition, December 2005.

GARSTKA, John J. *"O Desafio da Transformação"*, NATO Review, Primavera 2005.

HASTINGS, Michael. *"Who needs electrons?"*, Newsweek, 12 de Dezembro de 2005.

LEONHARD, Robert R. *"The levels of War"*, in Civilian Military Science 101-1, 2003.

LUCAS, Elisabeth. “*Reaping the Benefits of ICT – Europe’s Productivity Challenge*”, Market Report nº 342, Jul04.

PETERSEN, John L. “*Small Security: Nanotechnology and Future Defense*”, Defense Horizons, Março 2002.

PINTO, Cap Inf Carlos Alberto Nunes da Costa. “*A Gestão dos Sistemas de Informação e a GNR*”, in Pela Lei e Pela Grei Julho/Setembro 04, Lisboa, 2004.

PINTO, Rodrigues. “*Estratégia Operacional : O Que Está Além da Primeira Batalha*”, O Anfíbio, 2001, <http://www.cgcfm.mar.mil.br> – acedido em 21 de Setembro de 2005).

RAMALHO, TGen José Luís Pinto. “*O Conflito Assimétrico e o Desafio da Resposta- Uma Reflexão*”. Revista Militar nº 8/9, Agosto/Setembro 2005.

SANTOS, Cap Cav Sérgio Paulo Alves. “*O Exército Americano em Transformação*”, Revista Militar nº 8/9 - Agosto/Setembro 2004.

SANTOS, Eduardo Silvestre. “*Network Centric Warfare*”, [www.jornaldefesa.com](http://www.jornaldefesa.com) (acedido em 15 de Agosto de 2005) .

SANTOS, Gen Loureiro, “*Estratégia e Segurança Nacional na Era da Informação*”, Revista Militar nr 2445, Out05.

SZAFRANSKI, Richard. “*Uma Teoria da Guerra da Informação*”, [www.airpower.maxwell.af.mil](http://www.airpower.maxwell.af.mil). (acedido em 14 de Outubro de 2005)

TILFORD, Earl H. Jr. “*The Revolution in Military Affairs: Prospects and Cautions*”, Strategic Studies Institute, Carlisle Barracks, 1995.

VAZ, Nuno Mira, “*Reflexões sobre o Campo de Batalha no Século XXI*”, Nação e Defesa nº107, Primavera 2004.

WALKER, Karen: “*Net-Centric Vision*”, C4ISR Journal, Maio 2005.

### **Monografias**

CARREIRA, CorTm Dario F. Morais. “*Sistemas Inteligentes de Apoio à Decisão Tática*”. TILD CSCD 2003/2004, IAEM, Lisboa.

FERREIRA, CorTm Edorindo dos Santos. “*O Conceito de Network Centric Warfare. Implicações para a Transformação da Força Operacional Permanente do Exército*”. TILD CSCD 2004/2005, IAEM, Lisboa.

FERREIRA DE SOUSA, Maj Cav Francisco Xavier. *“Nível Operacional da Guerra: Conceptualização e Aplicação ao Caso Português”*. TILD CEM 1997/1998, IAEM, Lisboa.

NUNES, Viegas, *“O Impacto da Aplicação do Conceito Network Centric Warfare na Forças Armadas Portuguesas – Subsídios para o Levantamento de Uma Capacidade Centrada em Rede”*, Academia Militar, Novembro 2005.

SCHECHTMAN, Gregory M. *“Manipulating the OODA Loop: The Overlooked Role Of Information management n Information Warfare”*, USA Air University, Dezembro 1996.

VIEIRA, CorInf Victor Manuel Amaral, *“Componente Operacional do Exército Português. Que Modelo para o Futuro”*, TILD CSCD 2003/2004, IAEM, Lisboa.

### **Manuais**

(NC 20 – 77- 01), *“A ArteOperacional - Operações Conjuntas e Combinadas”*, IAEM, 2000

FM 100-5 – Operações, Maio 1986.

### **Legislação e Documentos Oficiais**

Conceito Estratégico de Defesa Nacional (Resolução do Conselho de Ministros n.º 6/2003, de 20 de Janeiro).

Conceito Estratégico Militar (confirmado em CSDN de 15 Janeiro de 2004).

Directiva 5/CEMGFA/2001, Directiva para as Forças de Reacção.

NNEC Data Strategy, ACT, Dec2004.

Plano de Médio e Longo Prazo do Exército, EME, Agosto de 2005.

### **Outros Documentos**

Conceito de Battlegroup da UE, Comité Militar da UE, 14 Junho 2004.

JOINT VISION 2020, Departamento da Defesa dos Estados Unidos da América.

TELO, António José, *“Portugal e a Transformação da Defesa”*, intervenção na Academia Militar, Janeiro 2003.

Documento A/1899 do Defence Committee da WEU, de 12 de Maio de 2005

### **Sites da Internet**

<http://www.leavenworth.army.mil>

[http:// www.jornaldefesa.com](http://www.jornaldefesa.com)

<http://www.carlisle.army>.

<http://www.cgcfm.mar.mil.br>

<http://www.dodccrp.org>

<http://www.airpower.maxwell.af.mil>

<http://www.nnec.act.nato.int>

### **Entrevistas**

TGen Reis, Comandante da Academia Militar, em 30Nov05

TenCor Barbas, Sub-Director do CIE, em 12Dec05

## Apêndice A : Glossário de Conceitos

**Arte Operacional** –O emprego de forças militares para alcançar objetivos operacionais e/ou estratégicos, por meio da concepção, organização, integração e condução de campanhas estratégicas, grandes operações e batalhas. A arte operacional traduz a estratégia dos Comandos Combinados numa concepção operacional e, por fim, em ação táctica, integrando as atividades chave de todos os níveis da guerra ” (Joint Pub 5-0)

**Auto-sincronização** – aptidão de uma força bem informada para organizar e sincronizar as complexas acções militares de baixo para cima, com base nas intenções do comandante superior, na unidade de esforço e em rigorosas regras de empenhamento. Segundo o DoD dos EUA, é a “capacidade das forças de baixos escalões operarem de forma quase autónoma e de redireccionar os seus esforços e actividades, através da exploração da compreensão da intenção do comandante superior”. (Rumsfeld, Donald H. “*Transformational Planning Guidance*”, DoD, April 2003, em Alberts, 2003) .

(Self-synchronisation) - *a form of organisation contributing to dissolve the inflexible hierarchy of the traditional defence. Educated and trained mission-assigned units have therefore the possibility, in the network, to organise themselves in the best way, depending on the situation.* (Documento A/1899 do Defence Committee da WEU de 12 de Maio de 2005).

**Battlespace (Espaço de Batalha)** - *the environment, factors and conditions that must be understood to successfully apply combat power, protect the force or complete the mission. This includes air, land, sea, space and the included enemy and friendly forces, facilities, weather, terrain, the electromagnetic spectrum and the information within the operational areas and areas of interest.* [USA JP 3.0, 2003].

**Comando Operacional.** Comando Operacional é a autoridade conferida a um comandante para atribuir missões ou tarefas a comandantes subordinados, para projectar unidades e reatribuir forças, e para manter ou delegar o controlo operacional e ou táctico consoante as necessidades. Esta autoridade não inclui responsabilidades administrativas ou logísticas. Este grau de comando e controlo permite, ainda, ao comandante atribuir forças aos comandantes subordinados. (IAEM, NC 20 77 01).

**Comando e Controlo** - *The exercise of authority and direction by a designated commander over assigned forces in the accomplishment of the force’s mission. The functions of command and control are performed through an arrangement of personnel, equipment, communications,*

*facilities and procedures which are employed by a commander in planning, directing, coordinating and controlling forces in the accomplishment of his mission.* [NATO, 1988].

**Commercial Off-The-Shelf (COTS)** – designação genérica de produtos, equipamentos e sistemas comercializados ao público em geral e também usados a nível militar, sem modificações. O uso de produtos COTS está a ser obrigatório em muitos programas governamentais pelas poupanças que oferecem em termos de aquisição e manutenção (<http://en.wikipedia.org>).

**Common Operational Picture (COP)** – Imagem (normalmente *display* de computador) que contém informação relevante partilhada por mais que um comando. Permite o planeamento conjunto e facilita a obtenção da compreensão da situação operacional por todos os escalões. ([http://en.wikipedia.org/wiki/Common\\_Operational\\_Picture](http://en.wikipedia.org/wiki/Common_Operational_Picture))

**Conhecimento** – É a informação contextualizada, associada a uma experiência, que compreende uma estratégia, uma prática, um método ou uma abordagem (Dinis, 2005, 24).

**Compreensão** - É o resultado do processo de integração do conhecimento existente sobre um determinado aspecto ou área de interesse, permitindo sustentar as decisões e as acções ao longo do tempo de forma lógica e racional (Nunes, 2005, 23).

**Compreensão da situação** (*situation awareness*) – é o resultado de estar consciente de tudo o que acontece em redor do indivíduo e da importância relativa do resultado da observação do meio envolvente. Pode ser descrita como o conhecimento ou o modelo mental da situação envolvente.

Segundo Ferreira, (TILD CSCD 2004/2005), para que um conjunto de indivíduos da mesma organização tenham uma consciência semelhante de uma dada situação, com base nos mesmos dados, informação e conhecimento, é necessária formação similar e treino contínuo.

**Dados** (*data*) – elementos discretos, não organizados, compostos por números, palavras, sons ou imagens independentes, que podem ser facilmente estruturados, mas que por si só não conduzem à compreensão dum facto ou situação (Dinis, 2005, 23).

**Guerra da informação** - tudo o que se possa efectuar para preservar os nossos sistemas de informação, da exploração, corrupção ou destruição enquanto simultaneamente se explora corrompe ou destrói os sistemas de informação adversários conseguindo obter a necessária



vantagem de informação. (NUNES, Viegas. “A guerra da Informação”, Revista Militar, nº especial, SET1999).

**Informação** (*information*) - conjunto de dados que quando fornecido de forma e a tempo adequados melhora o conhecimento da pessoa que o recebe, ficando ela habilitada a desenvolver determinada actividade ou a tomar determinada decisão ( Dinis, 2005, 23).

**Informações** (*intelligence*) – produto resultante do processamento da informação.

**Interoperabilidade** - Capacidade dos sistemas, unidades ou forças fornecerem serviços e aceitarem serviços de outros sistemas, unidades, ou forças e utilizarem os serviços assim trocados, operando eficazmente em conjunto (Federal Standard 1037C e DoD MIL-STD-188).

**Intranet** - rede destinada a organizar e partilhar informação no interior de uma organização. Emprega tecnologias e aplicações comuns às da *Internet* (*browsers*, páginas *Web*, *e-mail*, *mailing lists*, *newsgroup*), mas é concebida primariamente para ser utilizada apenas por pessoas que trabalham dentro da organização (Ferreira, TILD CSCD 2004/2005).

**Largura de banda** – medida, expressa em hertz, do espaço ocupado no espectro de frequências por uma transmissão de dados (informação) de um equipamento electrónico para outro.

**Lock-in** – inovação tecnológica ou de procedimentos que fixa o consumidor a uma determinada solução técnica, produto ou fabricante. No SW é o exemplo do sistema operativo MS-DOS, e das aplicações do MS Office.

**Nanotecnologias** – tecnologias relativas a coisas menores que 100 nanómetros, em especial no que se refere à manipulação de átomos e moléculas.

**Network Centric Warfare** - NCW corresponde à adopção de uma nova forma de pensar - pensamento centrado na “rede” - e aplicá-lo às operações militares. NCW enfatiza o potencial de combate que pode ser gerado pela interligação efectiva resultante da “malha de redes” espaciais inter-conectadas no Teatro de Operações. É caracterizada pela possibilidade de forças dispersas geograficamente (consistindo em entidades) criarem um alto nível de partilha da Compreensão da Situação Operacional que pode ser explorada para auto sincronização e outras operações centradas na “rede” para alcançar a intenção do Comandante. NCW tem a ver com o comportamento humano e organizacional (Alberts et al., 1999).

**Nível Operacional** – O nível da guerra no qual as campanhas e as grandes operações são planeadas, conduzidas e mantidas, a fim de alcançar os objetivos nos teatros de operações. As atividades deste nível fazem a ligação entre tática e a estratégia, estabelecendo objetivos

operacionais necessários para alcançar os objetivos estratégicos, seqüenciando eventos para alcançar os objetivos operacionais, iniciando ações e aplicando os recursos para realizar e dar continuidade a esses eventos. Essas atividades implicam uma dimensão de tempo ou espaço maior do que a da tática; asseguram o apoio logístico e administrativo das forças táticas e proporcionam os meios pelos quais os sucessos táticos são explorados para alcançar os objetivos estratégicos” (DoD, Joint Pub 3-0).

**Revolução nos Assuntos Militares (RAM)** - uma alteração de monta / grande envergadura na natureza da guerra, provocada pela aplicação criativa de novas tecnologias que, em conjunto com alterações na doutrina militar e nos conceitos operacionais e organizacionais, modifica drasticamente o carácter e a condução das operações militares (Office of Net Assessments do gabinete do Secretário da Defesa dos EUA).

**Sistema de Apoio à Decisão (DSS)** - Os Sistemas de Apoio à Decisão são sistemas de informação interactivos e flexíveis, baseados em computador, para gerir a tomada de decisão, no caso de problemas semi-estruturados (Turban, 1995, em <http://en.wikipedia.org>).

**Sistema de Informação (SI)** – um sistema automático ou manual, formado por um conjunto de pessoas, equipamentos, procedimentos e actividades, organizados para a recolha, processamento, armazenagem, transmissão e difusão de dados relevantes, às pessoas que dela necessitem (Federal Standard 1037C e DoD MIL-STD-188).

**Sistema de Informação e Comunicações (SIC ou CIS)** – conjunto de equipamentos, métodos, procedimentos e meios humanos organizados para levar a cabo o transporte da informação e o seu processamento.

**Superioridade de informação** – capacidade para recolha, processamento e disseminação de um fluxo de informação ininterrupto, mais rapidamente que o adversário, enquanto se reduz ou nega ao adversário a capacidade para fazer o mesmo. A superioridade de informação permite moldar o cenário envolvente de forma a este se adqur às nossas necessidades e objectivos. (Johan A. Goossens, C4I Division, ACT). De forma relativamente simplificada, a superioridade de informação é obtida quando um actor (competidor) supera os seus rivais no domínio da informação (Alberts et al., 1999).

**Tecnologias da Informação (TI) / Tecnologias de Informação e das Comunicações (TIC)** – conjunto de equipamentos e aplicações (*hardware* e *software*) relacionados com a tecnologia e todos os aspectos da gestão e processamento da informação em organizações de grandes dimensões ( <http://en.wikipedia.org>).

## **Apêndice B : Ilustrações**

### **ÍNDICE**

Ilustração 1	Níveis da Guerra.
Ilustração 2	Ciclo OODA
Ilustração 3.	Ciclo da decisão: Janela de Oportunidade
Ilustração 4	Sistemas de Informação.
Ilustração 5	Organizações e TICs: Relacionamento bi-direccional.
Ilustração 6	Evolução dos Sistemas de Informação.
Ilustração 7	As tecnologias da RAM actual.
Ilustração 8	Inovação versus Organização e Processos.
Ilustração 9	Modelo de Yetton.
Ilustração 10	Modelo de Yetton, corrigido.
Ilustração 11	Modelos de partilha de informação.
Ilustração 12	NNEC
Ilustração 13	NNEC- modelo físico e lógico
Ilustração 14	NNEC – enquadramento conceptual
Ilustração 15	A Soma das Partes
Ilustração 16	Modelo de Transformação das Forças
Ilustração 17	Elementos essenciais de combate
Ilustração 18	Conceito TIDE
Ilustração 19	O SIG
Ilustração 20	A Intranet da Defesa

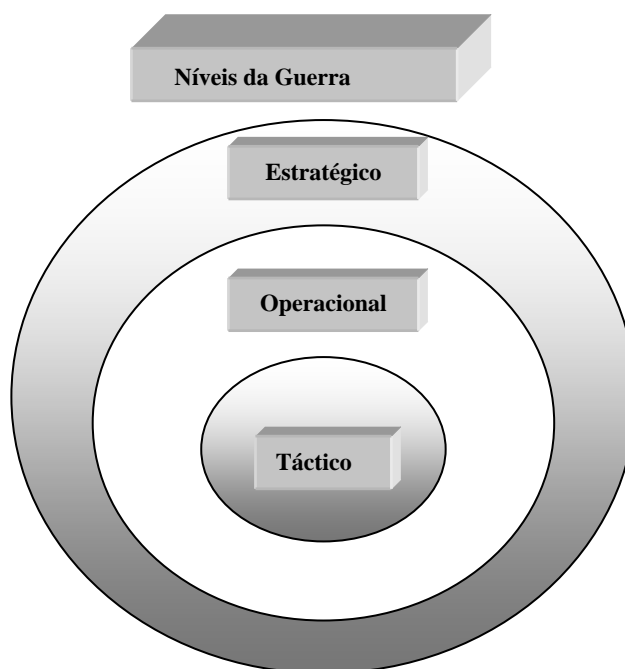


Figura 1. Os níveis da Guerra

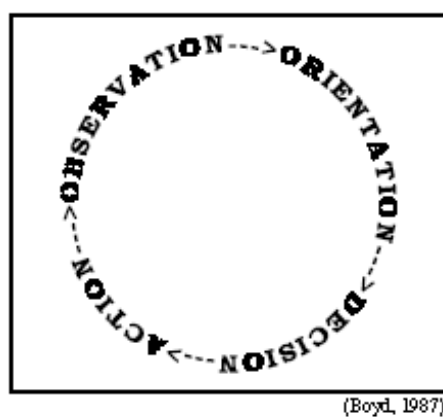


Figura 2. O ciclo OODA (fonte: Schechtman, 1996)

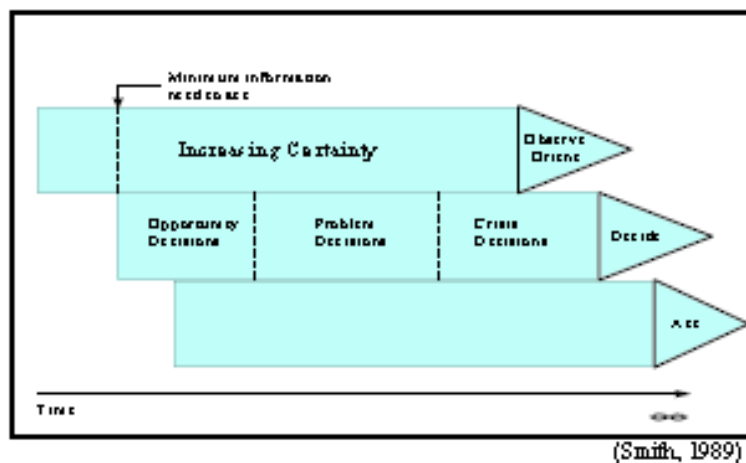


Figura 3. Ciclo da decisão : Janela de Oportunidade (fonte: Schechtman, 1996)

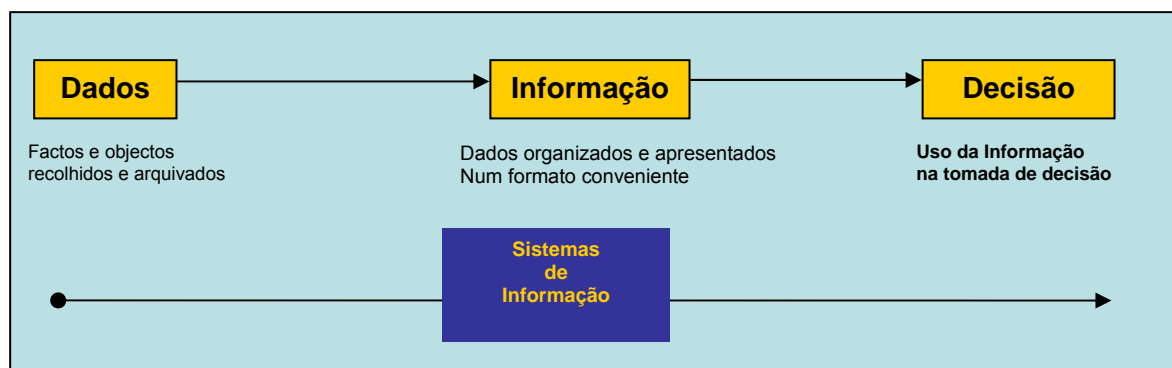


Figura 4. Sistemas de Informação (fonte: Pinto, 2004, www.gnr.pt)

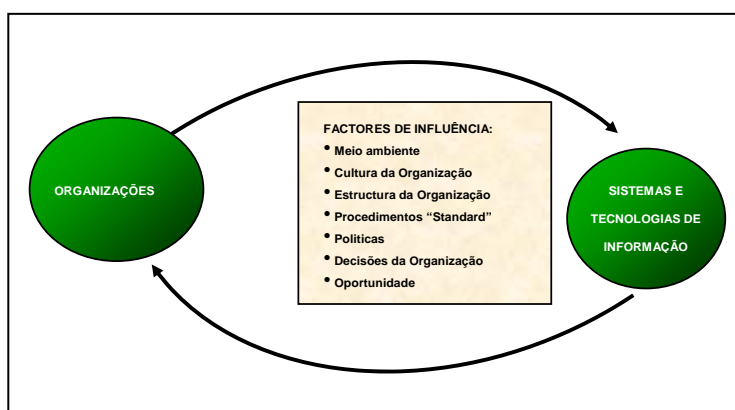


Figura 5. Organizações e TICs: Relacionamento bi-direccional (adaptado de Carreira, Dario. Apresentação IESM 16Nov2005)

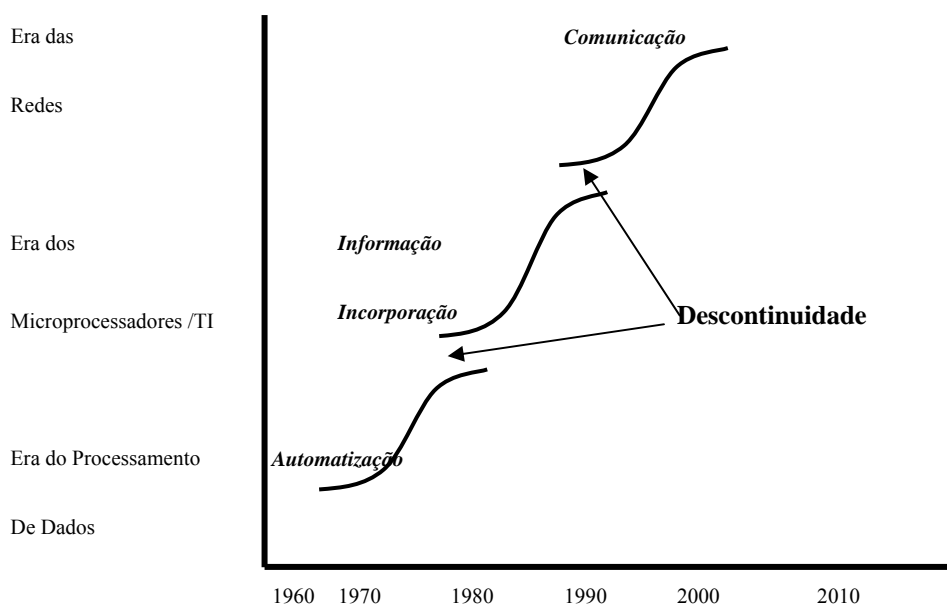
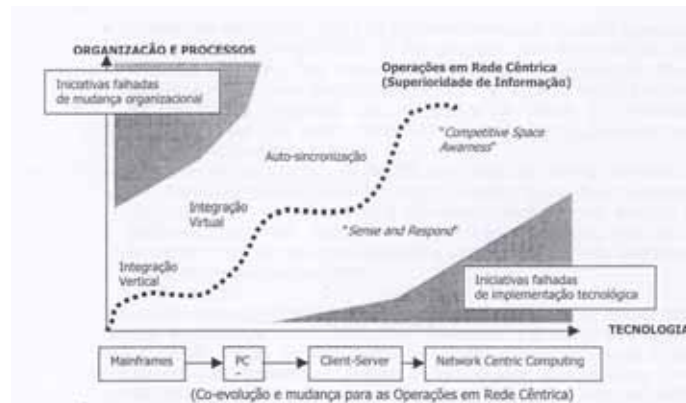


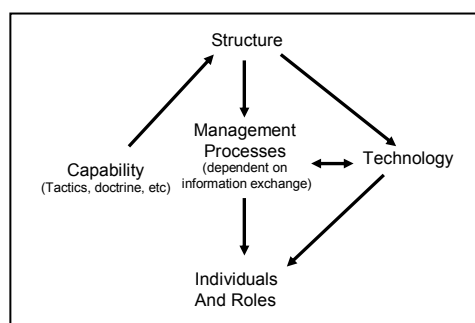
Figura 6. A evolução das TIC (adaptado de Mutsaers 1997 e Dinis 2005)

<b>Conceitos Operacionais</b>	<b>Actividade Operacional</b>	<b>Tecnologias</b>
Manobra dominante	Projecção da Força	Comunicações celulares globais “Pagers” inteligentes Preparação do Campo de Batalha pelas informações Materiais mais leves Simulações
	Operações decisivas	Dissimulação (“stealth”) Sensores guarnecidos Sensores de comando remoto Aviónicos avançados Veículos de grande mobilidade Tecnologias da guerra da informação Integração horizontal de tecnologia Digitalização Simulações
Protecção total	Preparação do Campo de Batalha	Algoritmos de inteligência artificial Catalogação de assinaturas Identificação do combatente Processamento directo nos sensores Munições inteligentes
Logística focalizada	Protecção da força	Tecnologias avançadas para o soldado Conjuntos de protecção química e biológica Melhorias na redução da assinatura Percepção da situação Tecnologias avançadas de identificação
	Sustentação da força	Tecnologias de informação para controlo de inventário Materiais mais duráveis Diagnóstico e reparação do software à distância Controlo automático de níveis e re-roteamento automático
Superioridade de informação	Domínio da informação	Comunicações sem fios Compressão de dados Tecnologia avançada de redes Transceptores de satélite móveis e muito pequenos Equipamentos com segurança multinível

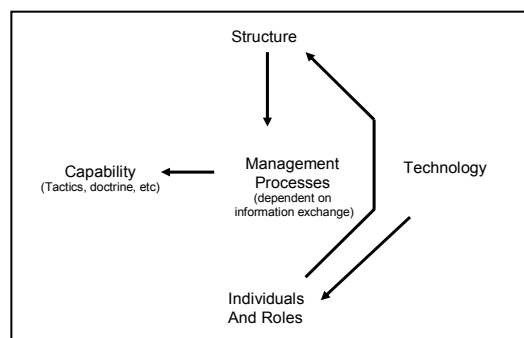
**Figura 7. As tecnologias da actual RAM** (fonte: MGen Carlos Alves, apresentação no Seminário sobre Guerra da Informação na Academia Militar, Abril 2004)



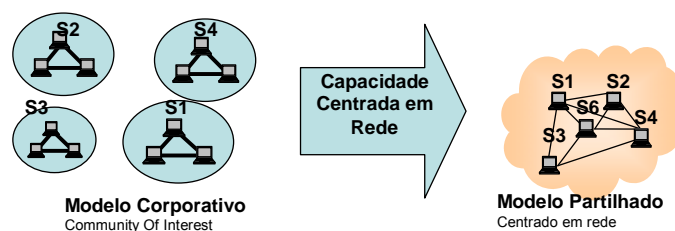
**Figura 8. Inovação versus Organização e Processos** (adaptado de Ribeiro, CFR João M. Fonseca, Info 24-DF-1/DICSI de Fev2004).



**Figura 9. Modelo de Yetton** (fonte: Potts,2003,34)



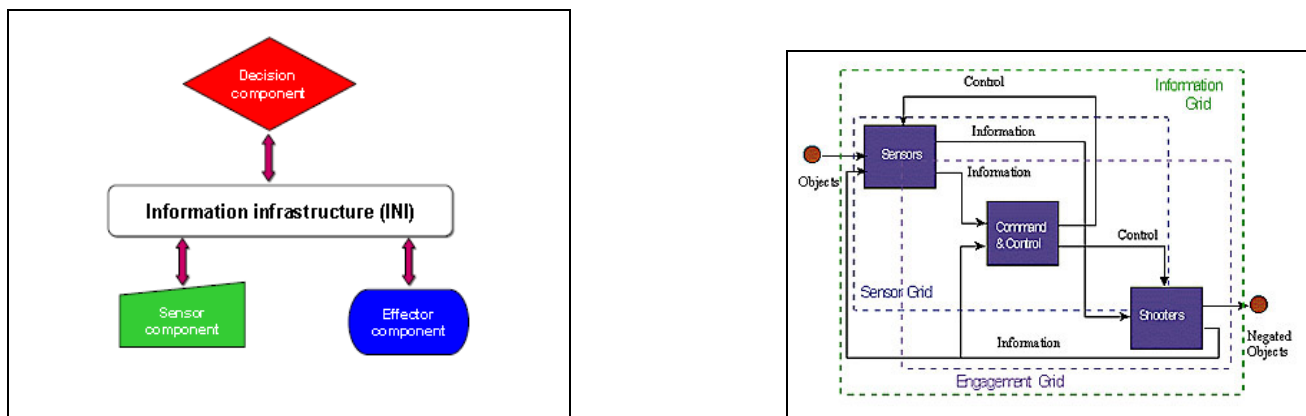
**Figura 10. Modelo de Yetton, corrigido** (fonte: Potts, 2003, 36)



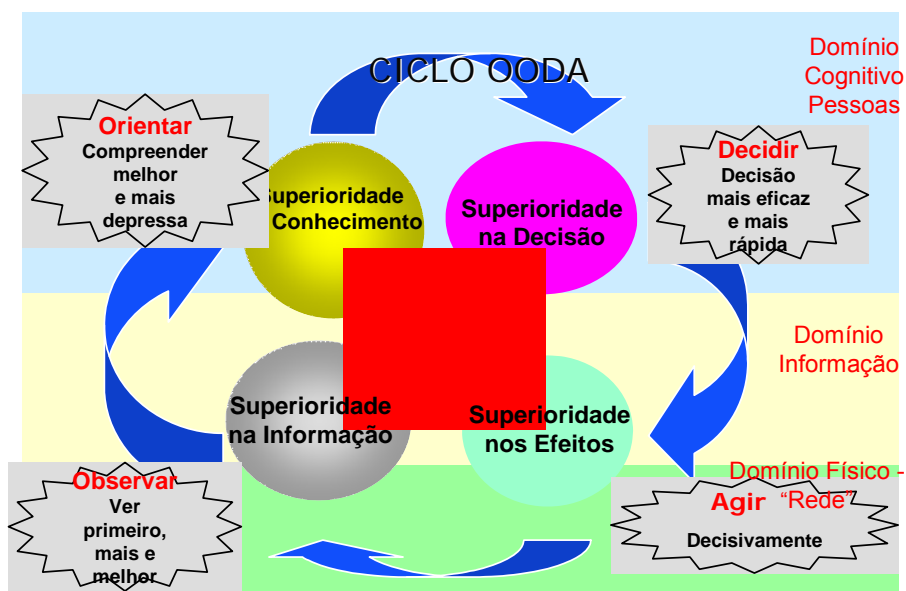
**Figura 11. Modelos de Partilha de Informação**



**Figura 12.** NNEC (adaptado da conferência NNEC Data Strategy, ACT, Dec2004)



**Figura 13.** NNEC- Modelos Físico e Lógico (fontes: Alberts, 1996 e Cebrowski, 1998 )



**Figura 14.** NNEC – Enquadramento Conceptual (adaptado de Bukman, ACT, 2003)



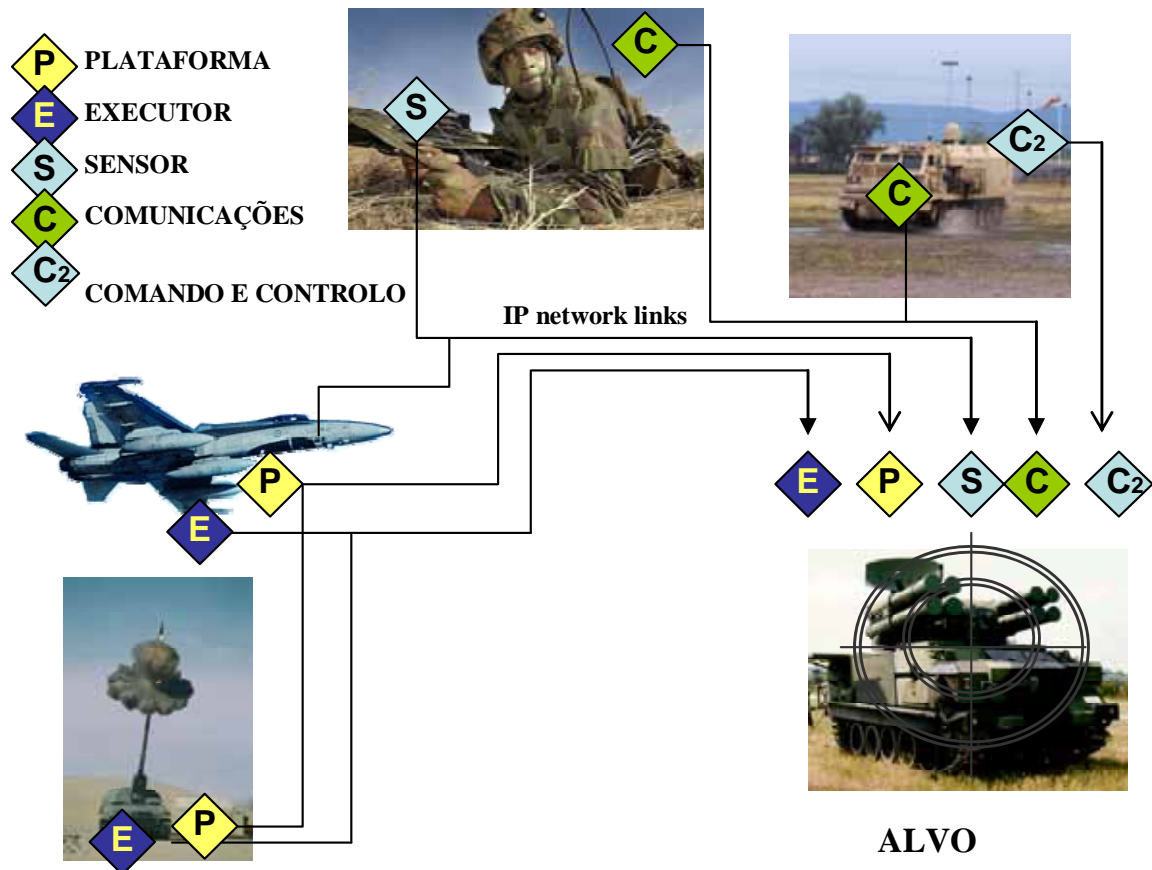


Figura 15. A Soma das Partes (fonte: John Bretschneider, C4SIR Journal, May2005)

Níveis da Guerra	Capacidade NCW componentes	Áreas de Transformação		
COGNITIVO	Pessoas	Liderança Formação CAX	INTEROPERABILIDADE	RELACIONAMENTO COM A INDÚSTRIA NACIONAL
INFORMAÇÃO	Processos	Doutrina Procedimentos		
	Organização	Unidades de Tm Unidades ISTAP		
FÍSICO	Tecnologia	Info-estrutura Sistemas de Comunicações Sistemas de Informação Portal		

Figura 16. Modelo de Transformação das Forças

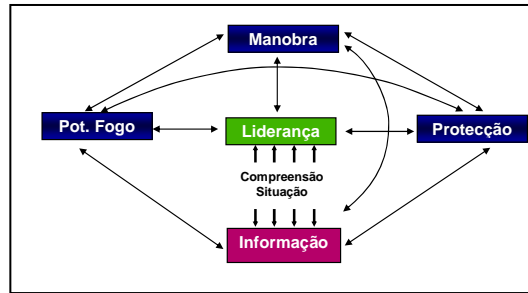


Figura 17. Elementos essenciais de combate (fonte: FM 3.0)

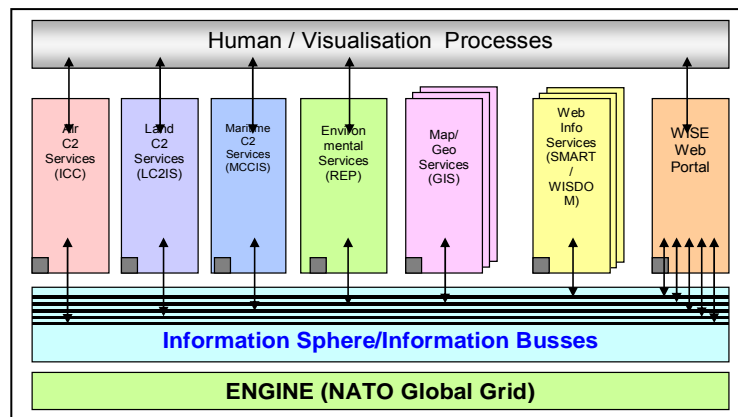


Figura 18. Conceito TIDE (adaptado de Bi-SCTransformation Conference, 2003)



Figura 19. O SIG (fonte: SAP)

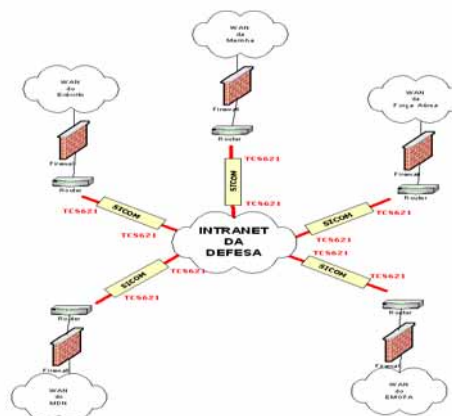


Figura 20. A Intranet da Defesa (fonte: CIE)

## Apêndice C : O Caso Português

### 1. Portugal e o Nível Operacional da Guerra

No caso Português, dadas as dimensões reduzidas do território nacional, não se pode falar, com propriedade, de operações no nível operacional. Historicamente e pela sua dimensão, Portugal actua ao nível tático, tendo tido no passado algumas incursões no nível estratégico.

As intervenções militares na Europa no Séc. 18 (guerra da Sucessão de Espanha e Campanha do Rossilhão) são intervenções que se inserem na esfera estratégica, uma vez que estavam em causa o alcançar posições estratégicas mais favoráveis na Europa, reforçar a capacidade de intervenção de Portugal e fortalecer as fronteiras com Espanha (Borges, 2000,18).

Já as operações da guerra do Ultramar podem inserir-se no contexto do nível operacional da guerra, salientando-se de entre estas a Operação Nó Górdio, em Moçambique. Dirigida contra o dispositivo de Cabo Delgado, da FRELIMO, foi a maior operação realizada nos três Teatros de Operações (Guiné, Angola e Moçambique) durante todo o período da Guerra, sob o comando do General Kaulza de Arriaga.

Assim, e no extremo estratégico, a definição dos objectivos do Estado, a elaboração do Conceito Estratégico de Defesa Nacional (CEDN) e do Conceito Estratégico Militar (CEM) dele derivado, bem como a definição das missões das Forças Armadas (MIFA) e o mais importante a declaração do estado de guerra, são competências dos órgãos Presidente da República, Assembleia da República, Governo e Conselhos Superior de Defesa Nacional (CSDN), Conselho Superior Militar (CSM) e Conselho de Chefes de Estado Maior (CCEM). Cabe-lhes ainda a elaboração dos planos de campanha das operações conjuntas e combinadas.

Descendo para o patamar operacional, mas ainda numa zona que se pode considerar de sobreposição dos níveis estratégico e operacional encontra-se o CEMGFA, e os seus órgãos de apoio e Estado Maior, ao qual compete genericamente elaborar o projecto de Conceito Estratégico Militar bem como planear, dirigir e controlar o emprego das Forças Armadas (FA) no cumprimento de missões e tarefas operacionais.

Por sua vez, a Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA), estabelece no artº 6º que o CEMGFA “*responde em permanência perante o Governo, através do MDN, pela prontidão, disponibilidade, sustentação e emprego das forças e meios que constituem a componente operacional do sistema de forças*” e “*exerce o comando operacional das Forças Armadas em tempo de paz*”. Para a sua concretização o CEMGFA dispõe dos comandantes operacionais (Açores e Madeira) bem como dos comandantes-chefe, que lhe compete nomear em tempo de guerra, para exercer o comando operacional das forças<sup>48</sup>.

De acordo com a Directiva 5/CEMGFA/2001, Directiva para as Forças de Reacção, o

---

<sup>48</sup> Lei nº 29/82 de 29Dec, “*Lei da Defesa Nacional e das Forças Armadas*”alterada pela Lei nº 18/95 de 12jul95.

CEMGFA prevê a atribuição do comando operacional da Força de Reacção Imediata ao Comando Operacional do Ramo melhor qualificado, de acordo com a especificidade da missão. Este aspecto é susceptível de criar dificuldades de relacionamento inter ramos, bem como conflitos de comando, uma vez que existe uma dependência do comando operacional do respectivo Chefe de Estado-Maior.

Finalmente ao nível tático, encontram-se os comandos das forças<sup>49</sup> a quem compete comandar as respectivas unidades e planear e executar as operações de acordo com as directivas e planos operacionais. Na Fig. 1, apresentam-se os níveis adaptados para a dimensão nacional.

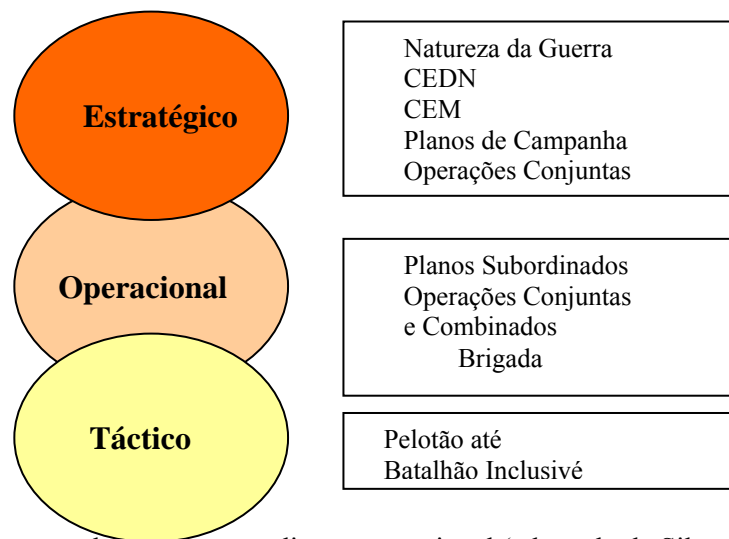


Figura 1. Níveis da guerra adaptados para a dimensão nacional.(adaptado de Silva, Esteves, A *Liderança e o Processo de Formação de Líderes*, CSCD 04/05)

No caso Português o espectro de missões previsível será cada vez mais o empenhamento em acções de cooperação técnico-militar no quadro da CPLP e participação em cenários de projecção de forças no exterior (FND) integradas com os aliados na NATO, União Europeia e Nações Unidas.

No interior do território nacional serão de esperar missões viradas para o apoio às populações, no âmbito da protecção civil e de combate a calamidades naturais, em paralelo com operações de combate ao terrorismo.

## 2. Operação Nó Górdio

Dirigida contra o dispositivo da FRELIMO em Cabo Delgado, Moçambique, a operação NÓ GÓRDIO foi a maior operação de guerra convencional realizada nos três teatros de operações (Guiné, Angola e Moçambique) durante todo o período da guerra colonial.

---

<sup>49</sup> Decreto Regulamentar 47/94, “Atribuições, organizações e competências dos Comandos Territoriais e das Tropas Aerotransportadas”, de 02Set94.

## 2.1 O Objectivo

O objectivo operacional da operação era o de acabar com a guerra através do aniquilamento do inimigo e libertação das populações, de modo a realizar-se o objectivo estratégico atribuído ao Comandante-Chefe, de restabelecer a paz, a lei e a ordem na província.

A operação foi dirigida contra o planalto de Mueda, local onde a Frelimo tinha a sua maior concentração de forças e meios - bases centrais, estruturas de comando, de apoio de fogos e apoio logístico. Acrescia ainda que esta zona gozava da imagem de “santuário”, onde as tropas portuguesas não tinham acesso, donde a importância psicológica acrescida da sua destruição, pelo impacto que teria sobre o moral do inimigo.

## 2.2 A Operação

A operação, conjunta, envolveu 8000 homens, dos três ramos das Forças Armadas, elementos de forças especiais (os Grupos Especiais, criados a partir das milícias da administração colonial) e o apoio de agências governamentais, como a DGS (Direcção Geral de Segurança).

O dispositivo inimigo apoiava-se na vizinha Tanzânia, a partir da qual a Frelimo recebia o apoio logístico e de reabastecimento necessário à continuação da sua actividade. Este apoio era canalizado para Moçambique através de diferentes infiltrantes, das quais a mais importante era a que se apoiava no complexo das Bases Limpopo 1 e Limpopo 2, próximas do rio Rovuma e a Base Beira, mais a sul.

As bases centrais eram a Base Moçambique, onde se encontravam os órgãos de comando, a Base Gungunhana onde se concentravam as armas pesadas e a Base Nampula, de menor importância. Neste local convergiam ainda as grandes vias de comunicação, de ligação ao mar, de ligação ao norte (Tanzânia) e das de penetração para sul, para o interior da província.

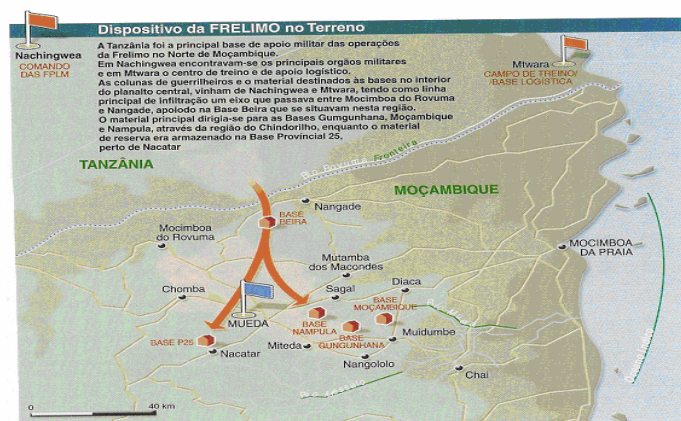


Figura 2. Dispositivo da Frelimo ( fonte Gomes, 2002, 39 )

A operação decorreu entre Junho e finais de Agosto de 1970, mas a sua preparação teve início em Dezembro de 1969, com a criação do Comando Operacional das Forças de Intervenção (COFI), constituído por elementos do Exército, Marinha e Força Aérea junto do QG do General

Kaulza de Arriaga, em Nampula, com a finalidade de planear e comandar a execução da operação.

Após a activação do COFI procedeu-se à concentração de meios (forças combatentes, de engenharia e de artilharia, viaturas blindadas, aviões e helicópteros) e à preparação dos itinerários em direcção ao objectivo. Esta actividade obrigou à construção e melhoramento de pistas de avião e de estradas, à aquisição por meios expeditos de equipamentos de comunicações, ao acondicionamento de viaturas inoperacionais e obuses de artilharia obsoletos, á recuperação de tendas, cozinhas, material de frio e instalação de um hospital de campanha em Mueda.

### 2.3 A Execução

O conceito do General Kaulza de Arriaga, era o de efectuar uma operação de cerco e destruição, seguida da ocupação do local.

O início da operação foi precedido da destruição e impedimento das linhas de comunicação com a Tanzânia, através da realização de uma operação, de nome de código “Dureza”, efectuada por forças de comandos e pára-quedistas sobre a Base Beira. Iniciada a operação, o cerco ocupou uma linha descontínua ao longo de 140 Km para isolar as três bases principais, que constituíam os objectivos/pontos decisivos, tendo o assalto com o fim de destruir os complexos militares e político/administrativos, sido efectuado com o apoio de fogos terrestre e aéreos.

O assalto esteve a cargo de três agrupamentos, de Comandos, Pára-quedistas e Fuzileiros, tendo-se desenrolado em duas fases:

- Numa primeira fase, sobre as bases Moçambique e Gungunhana, por Comandos e Pára-quedistas;
- Numa segunda fase, sobre a base Nampula, por um agrupamento de Fuzileiros.

Em paralelo desenrolaram-se acções de guerra psicológica (Apsic).

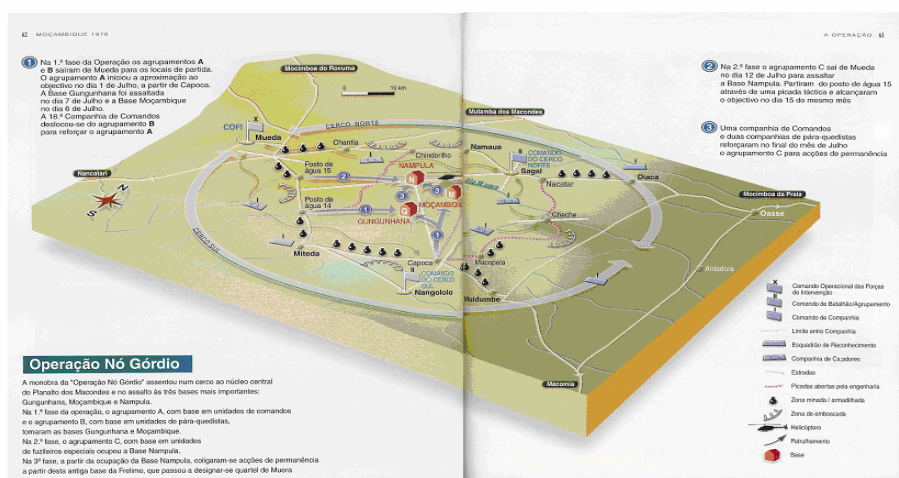


Figura 3. Operação Nó Górdio (fonte: Gomes, 2002, 62)

### 2.4 Análise

O NÓ GÓRDIO foi uma operação complexa, com uma componente logística de grande envergadura, que exigiu a construção e o melhoramento de vias de comunicação e de pistas de aviação, e o empenhamento de avultados meios terrestres, aéreos e navais, quer militares quer civis.

Foram constituídos propositadamente um Comando de Artilharia e um Comando de Transmissões para a realização da operação, envolvidas a 3ª Região Aérea, que forneceu o apoio aéreo de ataque ao solo, transporte tático, reconhecimento, reabastecimento e evacuação e ainda a Região Militar de Moçambique responsável pelo apoio logístico.

Se bem que o resultado final da operação tenha ficado aquém das expectativas, para o que contribuiu a reunião e movimentação dos apoios previamente ao lançar da operação, que alertaram o inimigo e lhe deram tempo para evacuar grande parte das bases principais, esta operação insere-se no nível operacional da guerra, porquanto nela se podem identificar claramente os conceitos que constituem a essência da arte operacional:

- Foram definidos objectivos político-estratégicos (reposição da paz, lei e ordem) que procuram atingir-se por recurso a acção militar, sendo o objectivo operacional a destruição e aniquilamento das forças da Frelimo. O uso da força militar foi feito com planeamento, organização e realização/condução da campanha. Foi criado o COFI para planear e comandar a operação, cujo objectivo era destruir o complexo militar da Frelimo no planalto de Mueda;
- Tratou-se de uma operação conjunta, com recurso a forças dos 3 ramos;
- Foi efectuada a concentração de recursos previamente à operação, o que obrigou à construção e melhoramento de pistas de avião e de estradas;
- Estiveram presentes os conceitos centro de gravidade (o conjunto das três bases centrais, onde se reuniam os meios militares, de comando e controlo e apoios de fogos e administrativo da Frelimo) pontos decisivos, manobra (combinação de cerco com ataques directos e indirectos, patrulhamentos e emboscadas) e criaram-se sinergias, patente na colaboração entre ramos e forças no terreno e o faseamento esteve bem definido;
- Foram identificados e previamente destruídos pontos decisivos –Bases LIMPOPO 1 e LIMPOPO 2 (Operação DUREZA) com forças dos Comandos e Fuzileiros.

Apesar de ser considerada uma operação bem conduzida, acabou por conduzir ao desbaratar de recursos escassos, logo pode ser igualmente considerada um erro.

Em Agosto 1970 as três bases estavam na posse das forças portuguesas. Mas em Setembro apenas permanecia uma, a base de NAMPULA, a menos importante mas a mais próxima de Mueda.



Após a operação constatou-se que as acções violentas realizadas pela Frelimo não tinham diminuído significativamente. O Relatório de Situação de Out70, relativo aos meses subsequentes à operação, refere:

*“ durante o período o In levou a efeito 729 acções, das quais 612 de minas. No trimestre anterior tinham sido 759 e 652 respectivamente. Destacam-se as seguintes acções ..... ataques a Omar com grande potencial de fogo de canhão sem recuo e metralhadora pesada, ....flagelação a Miteda com 100 elementos que só retiraram depois do emprego de heli-canhão e canhões sem recuo, ....ataque a Antadora com forte potencial de fogo”...*



## **Anexo A – Evolução das Tecnologias de Informação e Comunicações<sup>50</sup>**

A evolução da “informatização” nos Ramos seguiu a evolução tecnológica dos equipamentos. Os primeiros computadores eram volumosos, tinham consumos de energia consideráveis e precisavam de sistemas de arrefecimento próprios. Como só as plataformas navais tinham dimensão física para suportar esses requisitos, a informatização iniciou-se, naturalmente, pela Marinha.

À medida que a tecnologia desenvolvia computadores com menores dimensões e exigências, (de energia e arrefecimento) foi possível instalar SI em aeronaves, e com a chegada da Internet e a recente e crescente miniaturização, a informatização chegou às plataformas terrestres. A tabela seguinte resume a evolução dos computadores desde o seu aparecimento.

### **EVOLUÇÃO DOS COMPUTADORES AO LONGO DO TEMPO**

<b>Geração</b>	<b>Primórdios</b>	<b>Antecedentes</b>	<b>1ª</b>	<b>2ª</b>	<b>3ª</b>	<b>4ª</b>	<b>Futuro</b>
<b>Características</b>							
<b>Componentes</b>	Madeira Chapa	Relais	Válvula	Transístor	Circuito integrado	Microchip	Fibras ópticas? Módulos?
<b>Dimensão</b>	Sala	Sala	Armário	Gaveta	Placa	Pastilha	Pastilha?
<b>Velocidade (op/s)</b>	1	10 <sup>3</sup>	10 <sup>4</sup>	10 <sup>6</sup>	10 <sup>7</sup>	10 <sup>8</sup>	>10 <sup>10</sup> ?
<b>Data aproximada</b>	1890	1944	1944-52	1952-64	1964-74	>1974	20??
<b>Energia</b>	Manual Vapor	Eléctrica	Eléctrica (Kw)	Eléctrica	Eléctrica (100W)	Eléctrica (5W)	Luz? Enzimas?

**Fonte : IPAM Matosinhos**

### **1. As Redes**

São sistemas de comunicação de dados constituídos pela interligação de computadores e outros dispositivos, com a finalidade de trocar informação e partilhar recursos. Têm como objectivo:

- Partilha de recursos físicos, de periféricos que estejam ligados à rede, o que permite uma utilização mais eficiente e barata dos mesmos;

---

<sup>50</sup> Adaptado de IPAM, lições de Informática ao curso de Gestão de Marketing

- Partilha de programas e ficheiros, possibilitando a execução de programas e acesso a ficheiros que estejam noutros computadores ligados à mesma rede. Isto possibilita a vários utilizadores acederem a um mesmo programa ou ficheiro em simultâneo, de forma fácil e barata;
- Troca de informação, sob a forma de mensagens de correio electrónico e ficheiros de dados. Permite também a conversação directa, conferências e transferências de bases de dados;
- Melhor organização, com distribuição de tarefas e a possibilidade de trabalho em locais distantes, permanecendo os utilizadores ligados entre si através da rede.

Conforme a interligação dos computadores e a área em que se encontram existem vários tipos de rede, podendo ser quanto à área :

- Rede Local (**LAN** - Local Area Network) - uma rede que não tenha mais de 100 metros de comprimento e que existe normalmente dentro do mesmo edifício. Ex. rede escolar, sala de informática, rede dentro duma empresa.
- Rede Metropolitana (**MAN** – Metropolitan Area Network) - uma rede que abrange uma cidade inteira, interligando instituições e outras entidades.
- Rede de Campus (**Campus Network**) - uma rede que abrange uma serie de edifícios pertencentes a uma Universidade ou grande unidade fabril.
- Rede Alargada (**WAN** – Wide Area Network) - uma rede que abranja toda uma região, país ou mesmo a totalidade do globo, como é o caso da *Internet*.

Já quanto à Topologia Funcional, as redes agrupam-se em:

- Rede Cliente- Servidor (**Client-Server**) – uma rede, normalmente local, que possui muitos computadores “*cliente*” onde os utilizadores trabalham e utilizam os programas, e que possui um ou mais computadores “*servidor*” que fornece todos ou alguns programas, ficheiros e recursos necessários aos “*clientes*”. É o caso das redes em que se apoiam os Sistemas de Informação Militares que dispõem, tipicamente, de vários “*servidores*”, para ficheiros (*file server*), para bases de dados (*Database server*), para as comunicações e correio electrónico (*communications and mail server*) e para imprimir (*print server*).
- Rede Igual-para-Igual (**Peer-to-Peer**) – uma rede em que todos os computadores possuem normalmente os mesmos privilégios e em que todos possuem todos os programas e ficheiros para trabalharem sozinhos. Cada utilizador disponibiliza o

acesso aos recursos que entender que os outros possam aceder remotamente.

## 2. INTERNET

A Internet é uma gigantesca rede mundial de computadores interligados através de diversos meios de telecomunicação. A Internet, “auto-estrada da informação”, funciona como uma auto-estrada pela qual a informação sob a forma de texto, som e imagem é transmitida em alta velocidade entre qualquer computador ligado a essa rede.

A tecnologia e conceitos fundamentais utilizados pela Internet surgiram de projectos conduzidos ao longo dos anos 60 pelo Departamento de Defesa dos Estados Unidos, que visavam o desenvolvimento de uma rede de computadores para comunicação entre os principais centros militares de comando e controle que pudesse sobreviver a um possível ataque nuclear. Ao longo dos anos 70 e meados dos anos 80 muitas universidades ligaram-se a essa rede, o que contribuiu para diluir o carácter militar da rede e colocá-la numa direcção mais académica e cultural.

Em finais dos anos 80 a NSF – National Science Foundation dos EUA constituiu uma rede de fibra óptica de alta velocidade ligando centros de super-computação localizados em pontos chave no EUA. Essa rede da NSF, chamada de “ backbone da NSF”, teve um papel fundamental no desenvolvimento da Internet por reduzir substancialmente o custo da comunicação de dados para as redes de computadores existentes, que foram amplamente estimuladas a ligarem-se ao “ backbone” da NSF. O controle do “ backbone” mantido pela NSF terminou em Abril de 1995, tendo passado em sua grande totalidade para o controlo privado.

A Internet é um dos mais importantes e revolucionários desenvolvimentos da história da humanidade. Pela primeira vez no mundo um cidadão comum ou uma pequena empresa pode (facilmente e a um custo muito baixo) não só ter acesso a informações localizadas nos mais distantes pontos do planeta como também – e é isso que torna a coisa revolucionária – criar, gerir e distribuir informações em larga escala, no âmbito mundial, algo que somente uma grande organização poderia fazer usando os meios de comunicação convencionais.

Hoje em dia a Internet é uma teia (de onde ser conhecida por “web”) gigantesca, interligando praticamente toda a humanidade, com profundas implicações na economia, na partilha do conhecimento e na difusão das diferentes culturas.

A forma mais vulgar de explorar as suas potencialidades é feita através dos websites, dos motores de busca (*browsers*), dos serviços de correio electrónico, dos “Chat-rooms”, e mais recentemente dos “portais”, onde estão integrados os serviços atrás referidos.

### 3. Os Sistemas de Informação no Exército

Em finais dos **anos 60**, foi instalado um computador central nas instalações da Graça, para processamento essencialmente das aplicações de Recrutamento e Vencimentos.

Tratava-se de um processamento centralizado, essencialmente *batch*, e em que os dados eram inseridos nesse sistema por pessoal dos Serviços Mecanográficos do Exército. Só 10 anos mais tarde apareceram os primeiros terminais locais, que não possuíam qualquer capacidade de processamento local, e só na **década de 80** se instalaram os primeiros terminais remotos.

Entretanto, foram adquiridos pelo Exército outros sistemas de médio porte para apoio a alguns órgãos funcionais, a arquitectura física dos Sistemas de Informação torna-se mais complexa e, nos **anos 90**, o Centro de Informática do Exército mantém uma plataforma *Mainframe* para apoio às operações de Recrutamento e Pessoal e aposta em plataformas distribuídas com base em Computadores Pessoais para chegar às U/E/O's com aplicações que suportem as suas tarefas diárias (o Projecto RRING).

O projecto RRING, que deu corpo a esta nova realidade, fez crescer, congregou os esforços e orientou os investimentos de forma a que hoje o Exército possui uma rede corporativa que cobre todas as suas UEOs e se constitui como uma possibilidade para os órgãos superiores projectarem a sua capacidade de Comando.

Foi assim crescendo um conjunto de subsistemas de informação, nas proximidades dos órgãos que apoiavam, destinado a responder às suas necessidades específicas, feitas à medida destes órgãos e normalmente não preocupados uns com outros.

#### 3.1 A Nova Vaga de Sistemas Informáticos

Em **1998**, fica disponível um serviço de correio electrónico e o primeiro Portal com duas vertentes: uma interna conhecida como Intranet e outra na Internet.

Este tipo de solução apresenta como argumento mais favorável a utilização da Rede como um meio de comunicação entre os diferentes sistemas na organização: pessoal, logística, financeiro.

Em **2000**, foi instalado no Agrup C/KFOR um servidor de correio electrónico ligado directamente à Rede de Dados do Exército, através de um router colocado no Kosovo, permitindo assim uma maior aproximação das Forças Nacionais Destacadas à estrutura permanente do Exército. Esta solução seria implementada posteriormente na Bósnia e em Timor.

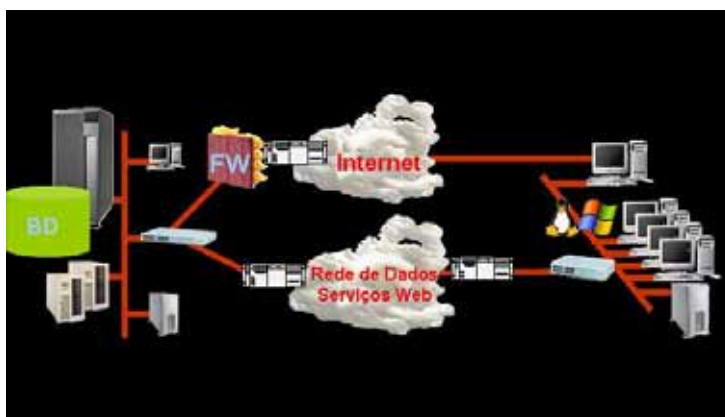
Durante este mesmo ano, com o alargamento da Rede de Dados e a introdução de ferramentas orientadas para a Web, foi desenvolvido o Portal destinado à partilha de

informação na Intranet, foi generalizado o serviço de correio electrónico, e procedeu-se à inauguração do Portal do Exército na Internet em Julho de **2002**.

Actualmente, a Intranet do Exército estende-se por todo o território continental, e pelos arquipélagos dos Açores e Madeira, Bósnia, Kosovo, Afeganistão e em todos os Teatros de Operações em que existam Forças Nacionais Destacadas.

Actualmente com mais de 10 000 utilizadores registados, a Intranet é constituída por 4791 estações de trabalho e 217 servidores, existindo 8015 contas de e-mail pessoal e 577 oficiais.

Em **2005** foi criado o serviço de WEBMAIL integrado com a Internet, o qual passou a permitir o acesso remoto a partir da Internet às contas de e-mail internas.



Rede de Dados do Exército

## Anexo B – Revoluções nos Assuntos Militares

As RAM destes dois últimos séculos assentaram em desenvolvimentos na química que alteraram drasticamente o alcance e a cadência de tiro das armas utilizadas na I e na II GM, e em desenvolvimentos na química e na física avançada que conduziram ao domínio do voo, à melhoria nas transmissões rádio e ao aparecimento dos radares. Culminaram com o desenvolvimento das tecnologias de fissão e fusão nucleares, que deram origem às armas nucleares. Estas, por sua vez, foram o factor determinante das organizações militares no período subsequente, graças à sua influência no estabelecimento das doutrinas de destruição mútua assegurada (MAD) e ao período da guerra fria que se seguiu até ao desmantelar da União Soviética.

As RAM mencionadas são designadas por RAM de “efeito combinado” ou de “sistema combinado”, porquanto assentam na reunião/conjugação de vários sistemas de armas diferentes, encarados sob novas perspectivas e utilizados de forma inovadora para criar um efeito final revolucionário.

Já às RAM que assentam numa única tecnologia, de tal forma revolucionária que por si só tenha sido capaz de condicionar o modo como a sociedade e os militares passaram a funcionar, chama-se RAM de “sistema único”. Exemplos desta última são a pólvora e a revolução nuclear que transformaram a forma de fazer a guerra.

Relativamente à RAM que agora se inicia, Steven Metz considera que esta se articula em dois patamares (Fig 1), caracterizando-se o primeiro patamar, o actual, pela predominância das plataformas, armamento com guiamento de precisão, sistemas de comunicações e informação, forças conjuntas e combinadas e conceitos como o ataque aos centros de gravidade. A segunda fase desta RAM verá já um campo de batalha dominado pela robótica e nanotecnologia, e pelo aparecimento de “armas inteligentes” aptas a decidir quando e onde actuar (Metz, 1995).

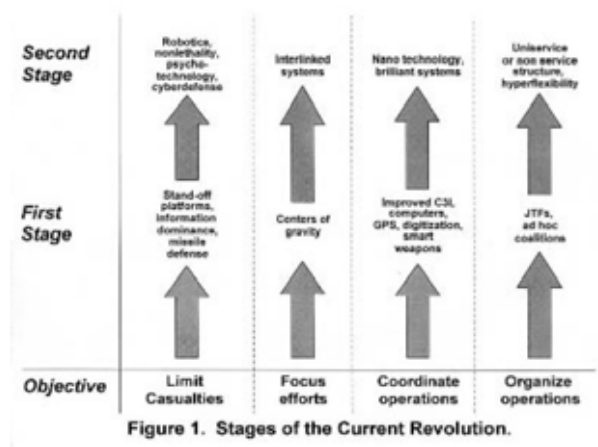


Figure 1. Stages of the Current Revolution.

(Fonte : Metz, 1995, 6)

Recentemente, os EUA determinaram que todos os telefones celulares ali comercializados sejam equipados com GPS, de modo a possibilitar a localização dos respectivos proprietários. Ao mesmo tempo está em estudo o uso de dispositivos designados por Individual Position Locator Device (IPLD), destinados a monitorizar a localização de cidadãos na perspectiva de terem de ser retirados de um país estrangeiro no decurso de uma Noncombatent Evacuation Operation – NEO (Metz, Kivit, 1994, 4).

O IPLD é a consequência natural das pulseiras electrónicas usadas para controlar condenados a prisão domiciliária e poderá ser implantado sob a pele, monitorizado via GPS, podendo ser usado como dispositivo IFFN (identification Friend, Foe or Neutral).

Entretanto, no campo da tecnologia, investigadores na Universidade de Standfort, EUA, conseguiram, em Outubro de 2005, produzir chips que utilizam fotões, em vez dos electrões tradicionais. Embora possa demorar cerca de 5 anos até que haja soluções técnicas economicamente viáveis, é de esperar em 2010 uma nova geração de computadores, em que as ligações internas sejam feitas em fibras ópticas. Isto irá acelerar as velocidades de processamento num factor de 10 a 100. Haverá chips a processar 100 biliões de bits por segundo. Será então possível fazer down-loads de filmes em segundos e efectuar pesquisas quase instantâneas em bases de dados com gigabytes de informação, o que abre perspectivas ainda inimagináveis (Michael Hastings, “Who needs electrons?” Newsweek 12Dezembro2005, p. 55).

## Anexo C: Exemplos<sup>51</sup>

### Germany

The concept of network-centric operations (NetOpFü) is tied in closely with reforming German armed forces capabilities to make them better adapted to today's operational requirements and constraints. The development of a national concept takes account of the possibility of forms of bilateral and multilateral cooperation at the European and transatlantic levels.

The aim of transformation in the case of the Bundeswehr is to develop its expeditionary and forces projection capability, preferably in a joint multinational context. The present reform envisages the setting up of three joint forces by 2010: an intervention force, a stabilisation force and a force providing support to land forces (some 250 000 troops in total, 105 000 for the land army). Six major essential capabilities have been identified in the process, the first two of which are basic to network-centric operations. They are:

- "Command and Control;
- Intelligence collection and reconnaissance;
- Mobility;
- Effective engagement;
- Support and sustainability;
- Survivability and [force] protection".

Defence policy guidelines adopted in 2003 state: "Considering the security situation, there is no requirement to furnish all sub-capabilities with state-of-the-art, high quality material, nor are there the financial resources". Priority is to be given to capabilities that as yet do not exist, in particular "global reconnaissance" and "efficient interoperable command and control systems and means". These are two essential network-centric capabilities for setting up ISTAR groups around which Germany is to develop its NetOpFü capabilities.

Battalion-size ISTAR groups concentrate within them the range of intelligence-gathering and reconnaissance resources required to secure a COP more rapidly and efficiently than in the past: UAVs with optical observation and SIGINT systems, human intelligence and combat/reconnaissance vehicles with modern networked communications systems (Dingo, Fennek and Luchs vehicles). The use of SAR-LUPE satellite radar imagery will significantly strengthen those units by increasing their range of observation of the theatre of operations.

---

<sup>51</sup> Documento A/1899 do Defence Committee da WEU em 12 de Maio de 2005



In terms of C2 structures, current reforms envisage the setting up of "HERKULES", a wired and wireless communications system that will eventually integrate and connect up existing networks: the army's HEROS and FAUST systems; the navy's MHQ and MCCIS and the Luftwaffe's (air force) EIFEL/GAFCCIS (German Air Force Command and Control Information System) and the German Defence Ministry's RUBIN systems.

Another ongoing project is Standard-Anwendungs-Software-Produktfamilien (SASPF) a range of products, software and standardised computer applications for the armed forces being developed by the German group SAP. SASPF is intended to replace current systems (networks, software and applications) that are now either obsolescent or incompatible.

Training in joint formation constitutes a priority in developing the German armed forces network-centric capabilities. From 15-26 November 2004, an initial joint exercise took place at the Wilhelmshaven Naval Base, for verifying the capacity to produce and exploit a CROP (Common Relevant Operational Picture). The "Common Arrangement 04" exercise brought together naval, air force and land force units to validate concepts evolved by the Bundeswehr's Transformation Centre. The aim is ultimately to end up with an autonomous German capacity to produce and exploit a CROP by 2010.

## **France**

The Bulle Opérationnelle Aéroterrestre (Armée) (BOA) project, due for completion in 2025, is a demonstrator of France's new military technology capabilities present and future, with a three-pronged research and investment strategy focusing on information control, space-based assets and observation UAVs and UCAVs.

The BOA is based on the "combined action of a number of factors (manpower, vehicles, robots and UAVs) that can simultaneously communicate, observe, provide information and act both through existing technologies and new technologies yet to be developed". It is essentially a reorganisation of France's (land) army based on the idea of "battlefield digitisation" but joint cooperation remains a possibility in the event of there not being total integration (although that would seem to be the aim in the American project through the Cooperative engagement and Global Information Grid concepts). The BOA is based on a range of assets: those existing (communications, aircraft, radar, satellites), currently being developed (UAVs, robots, the "soldier of the future") and to be defined in the near future (Directed Energy Weapons (DEW), such as, for example, Electromagnetic Pulse (EMP) and High Powered Microwave (HMP) Weapons).

Man-machine interaction is central to BOA, of which the first elements of the "Félin" soldier system programme come on stream in 2006-07. France will be the first European country to deploy a network-centric soldier, to meet national requirements and those of the NATO Response Force and European Union battlegroups. From 2015-25, BOA designers will also work on a concept for use, HOBOT, involving autonomous robots and human soldiers employed in close coordination. "Félin" consists of three principal systems: individual, specific and collective. The first has six different elements: clothes and other forms of protection, the portable electronic platform, individual energy sources, weapons, headgear and the "Félin" information network. The other two systems are concerned with means of communications/ navigation/positioning and of observation, and with batteries.

BOA is highly dependent on a space-based defence system made up of observation (Helios 1 or Helios 2), communication and navigation satellites (necessary for locating national, allied or enemy forces and for guided and precision munitions) and the capability to deploy UAVs and multi-mission robots, as sensors or for active or passive reconnaissance or defence. All of these systems, down to the vehicles and the "soldier of the future" will be linked via the high band-width communications networks necessary for transmitting all forms of real time data essential in building up the COP that any nation aspiring to lead a multinational or coalition operation must now have at its disposal.

The Helios 2A optical observation satellite, which was put into orbit in December 2004 and declared operational in April 2005, is one of the centrepieces of the whole system. Supplementing and enhancing the capabilities already provided by the Helios I satellites, its presence means that areas such as intelligence, preparation of missions and drawing maps of hitherto uncharted or imprecisely charted areas can now be covered. These three aspects, taken together, constitute ISTAR capabilities from which France's partners, Belgium and Spain, are able to benefit by means of this satellite. This approach has confirmed France's "umbrella" role in Europe in regard to the development of network-centric capabilities, also in evidence in the Franco-German "Tigre/Tiger" attack helicopter programme, designed from the outset to integrate with the BOA.

### **The United Kingdom**

The objective of the British concept of "Network Enabled Capability" (NEC) is "to enhance military capability by the better exploitation of information". Information is a power multiplier and NEC has been designed in that optic around four key notions: "sense, understand, develop intent, synchronise effects", or in other words around information sensors, COP, C2

networking and auto-synchronisation to achieve an optimum EBO on the theatre of operations. NEC is one of the main thrusts of the reform (transformation) of the British armed forces described in the "Defence White Paper 2003", and the "Defence Command Paper 2004", where it is stated that:

"NEC is about the coherent integration of sensors, decision-makers and weapon systems along with support capabilities. NEC will enable us to operate more effectively in the future strategic environment through the more efficient sharing and exploitation of information within the UK Armed Forces and with our coalition partners. This will lead to better situational awareness across the board, facilitating improved decision-making, and bringing to bear the right military capabilities at the right time to achieve the desired military effect. This enhanced capability is about more than equipment; we will exploit the benefits to be obtained from transformed doctrine and training and optimised command and control structures. The ability to respond more quickly and precisely will act as a force multiplier enabling our forces to achieve the desired effect through a smaller number of more capable linked assets".

The UK's network-centric capabilities are thus being developed via a raft of major programmes, either still in their initial phases or already being implemented by the armed forces. This is being done in three stages: initial (2007), transition (2015) and maturity (2020-30) which together form part of whole project known as "Network Integration Test and Experimentation Works" or NITEWorks, under the leadership of BAE Systems.

The United Kingdom is the only country to date to have experience of a network-centric operation under actual coalition conditions. This was Operation Telic, which formed part of the American Operation "Iraqi Freedom" carried out in March 2003. The first evaluations of this joint undertaking were published in 2004 and reviewed in 2005 in a report: "US/UK Coalition Combat Operations during Operation Iraqi Freedom" published by the US Defense Department's Office of Force Transformation in conjunction with the UK Ministry of Defence.

In order to be able to operate with the United States, British forces had to be equipped with American kit and were partially connected to the US network. They thus had access for the first time to the Force XXI Battle Command Brigade and Below (FBCB2)/Blue Force Tracker (BFT) systems, thanks to a loan of 47 kits (as against approximately 1 000 in service in US land army, Marine Corps and air force units). Communications were strengthened by the deployment of the Joint Operational Command System, of British origin, but which does not have the same capability as equivalent US systems.

In order to facilitate coordination and better integrate the British force into the US environment, a specific information system for the coalition - CENTRICS-X - was set up, but the

UK's dependence in intelligence terms became obvious from the fact that the SIPRNET system was operated in the British units under extremely strict procedural constraints imposed by US (Foreign Disclosure) officers.

Coordination between the two forces was effected generally without much difficulty, notwithstanding the short period of training the British troops had in working in coalition in a network-centric environment. So the BFT kits were not integrated into deployed assets until February. However, in some instances the two forces were unable to communicate and act in coordinated fashion and the "gap" in terms of technology, doctrine, training and profile of staff involved in so far as systems operators were concerned, served to illustrate the problems Europeans have to deal with if they want to interact with US forces in the near future.

In contrast, the US land forces deployed in OIF had more familiarity with computer-based systems - having already used tactical intranets, such as SIPRNET, to provide some INTEL and situational awareness for some time. Therefore, their TTPs are likely to have evolved somewhat towards those needed for digital situational awareness. This is likely to have made them more amenable to adapting to using FBCB2/BFT for a significant proportion of their situational awareness needs during OIF.

(...)

Due to their earlier exposure to the next technology wave (i.e. digital information that supports SA [situation awareness], such as tactical intranet and FBCB2/BFT) a larger proportion of the US forces are happy to migrate to this technology. By comparison, the bulk of the UK forces are still happiest with their proven technology and it is only a relatively small number who are prepared to try the new technology - largely in a tentative and experimental way".

## **Anexo D: Future Combat Systems**

O combatente de infantaria está no centro de uma das transformações mais drásticas da sua existência<sup>52</sup>. Quando o conceito *Future Combat System (FCS)* estiver operacional e quando as Divisões típicas da Guerra Fria se reciclarem em Unidades de alta tecnologia, moduláveis em “Forças por Objectivo”, o soldado levará para combate um sofisticado conjunto de equipamentos: computador com acesso permanente a informações (gráficas e sob a forma de texto) inscritas num ecrã integrado no aparelho de visão, o que lhe permite determinar em permanência a sua posição e a dos seus camaradas e fornecer em tempo real, aos órgãos de apoio de combate, as coordenadas das posições inimigas; arma individual que pode disparar sem interferência humana directa; capacete em material ultra-ligeiro, dotado de um sistema de suspensão que assegura a estabilidade dos instrumentos ópticos a ele agregados; e laser multi-funções que, entre outras capacidades, emite uma espécie de bilhete de identidade luminoso para as forças amigas.

Pela sua importância, apresenta-se em anexo um resumo do sistema de combate do futuro do Exército dos Estados Unidos, o qual os EUA consideram como sendo o garante da capacidade para o Exército poder cumprir a missão.

Esta informação é retirada do Army Transformation Roadmap de 2004, documento da responsabilidade do Deputy Chief of Staff americano, onde é exposta a estratégia para a transformação do Exército Americano e pormenorizadas as actividades a desenvolver para a aquisição das capacidades necessárias à execução de operações conjuntas pelas forças existentes. Detalha ainda as capacidades necessárias à futura “Joint Force” para garantir a superioridade na manobra terrestre.

O FCS, núcleo duro da futura unidade de manobra, é formado por 18 plataformas (tripuladas e não tripuladas) centradas em torno do combatente e integradas na rede de comando e controlo do campo de batalha. O FCS dará ao soldado conhecimento superior permitindo-lhe ver primeiro, compreender primeiro, agir primeiro e dar o golpe decisivo primeiro.

Até 2020 a estrutura de comando de Divisões, Corpo e EAC (escalão acima do corpo) vai ser substituída por 2 escalões de comando designados por UEx (com controlo táctico e operacional das Unidades combatentes) e UEy (que garante o fornecimento das capacidades ao comandante das forças conjuntas).

---

<sup>52</sup> BOOT, Max, *The New American Way of War*, Foreign Affairs, July/August 2003, vol. 82, nº4, pag 52

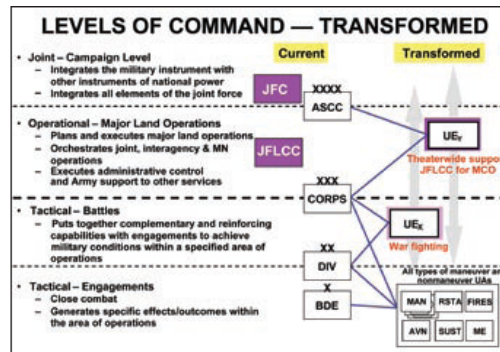


Figura1. Redistribution of Headquarters Functions,  
(Fonte : Army Transformation RoadMap, 6)

As UEx serão unidades autónomas, com capacidade de actuar em ambiente “net centric”, capazes de :

- Controlar desde 1 a 6 Brigadas de manobra (misto de Heavy, Infantaria e Stryker, equipadas com o FCS);
- Controlar uma mistura de funções (apoio de fogos, reforço de manobra, RSTA, apoio aéreo) através de brigadas multifuncionais, como descrito na fig 2.
- Organizar e distribuir módulos de comando e controlo de acordo com as situações;
- Funcionar como Quartel General de um Army LCC para operações de contingência de escala mais reduzida;
- Controlar operações de assalto aéreo com unidades desde escalão Batalhão a unidades de escalão Brigada;

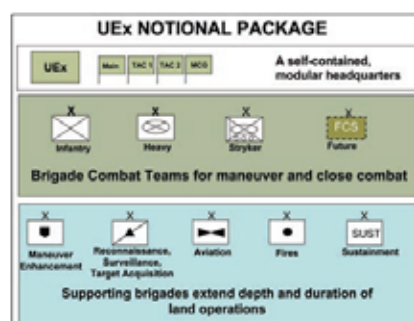


Figura2. Unidade Escalão X (UEx) (Fonte: Army Transformation RoadMap)

O futuro FCS assenta na existência de uma infraestrutura de comunicações (Global Information Grid - GIG) de que fazem parte as redes dos ramos (AirforceConstellation Net, Navy's Force Net e a LandWarNet). O principal problema/dificuldade é conciliar as expectativas de os utilizadores sedentos de cada vez mais informação com as limitações tecnológicas em termos de largura de banda e de aplicações disponíveis.

## FUTURE FORCE

The primary goal of Army transformation is the development of the Future Force — a strategically responsive, precision maneuver force that is dominant across the range of military operations. Balanced across a mix of light, medium and heavy formations and optimized for strategic versatility, this lighter and more agile force will dominate land operations in any future conflict. It will also perform seamless transitions from peacetime readiness to smaller-scale contingencies or major theater warfare. The ultimate measure of success of the Future Force, therefore, will be its contribution to future joint operations, in concert with interagency and multinational partners. In keeping with this fundamental guideline, the force is being designed to sharply expand the options available to the joint force — whether that is to swiftly defeat the efforts of regional aggressors, win decisively in extended conflict, or execute lesser contingency operations. The full-spectrum quality of this force will ensure its long-term relevance to adaptive, sophisticated threats and the frequently changing requirements of the emerging operating environment. The Future Force concept is founded on six main operational themes:

- Operational Maneuver from Strategic Distances is the rapid projection of modular, scalable, combined arms formations, tailored in force capability packages to meet the requirements of each contingency. Employing advanced lift platforms not dependent on improved ports, the Army will deploy much more rapidly into multiple points of entry and along parallel force flows to increase deployment momentum and close the gap between early-entry and campaign forces.

- Entry and Shaping Operations seize the initiative, shape the battlespace and set the conditions for decisive operations. Use of multiple entry points will help overcome enemy anti-access points, enhance surprise, reduce predictability, and, through the conduct of immediate operations after arrival, produce multiple dilemmas for the enemy.

- Intratheater Maneuver of Mounted Forces circumvents prepared defenses, extends the operational reach of the joint force commander, and exploits opportunities.

- Decisive Maneuver, as conducted by the Future Force, will rapidly achieve strategic ends. Decisive maneuver operations encompass:

- Simultaneous, distributed operations within a noncontiguous battlespace framework will fundamentally change the geometry of the enemy's defense and enables the Future Force to dislocate and defeat the enemy.
- Direct attack of key enemy strike and maneuver capabilities will accelerate the disintegration of the enemy defensive integrity.

- Continuous operations and increased operational tempo will overwhelm the enemy's capability to respond effectively, resulting in the physical destruction and psychological exhaustion of enemy forces.
- Network-Enabled Battle Command provides the required base of situational understanding for the most effective application of combat capabilities and forces and enables self-synchronizing forces to respond quickly to changing battlefield conditions.
- Distributed Support and Sustainment ensures freedom of maneuver with a minimum support and sustainment footprint throughout the battlespace.

## FUTURE COMBAT SYSTEMS

Although the Future Force will be a hybrid force, one of the key future elements of the hybrid mix will be the Future Combat Systems-equipped unit of action. The FCS-equipped unit of action encompasses more than a new set of capabilities. Rather, this organization reflects a fundamentally transformed method of combat. The core of the Future Force's maneuver unit of action is the Future Combat Systems, comprised of 18 manned and unmanned platforms centered around the Soldier and integrated by a battle command network. FCS will provide Soldiers with significantly enhanced situational awareness — enabling them to see first, understand first, act first and finish decisively.

The Future Combat Systems comprise a family of advanced, networked air- and ground-based maneuver, maneuver support and sustainment systems. FCS employs a revolutionary, integrated architecture to help meet the commander's requirements. These networked capabilities include networked communications, networked operations, sensors, battle command systems, training platforms, and both manned and unmanned reconnaissance and surveillance capabilities. These will enable improved situational understanding and operations at a level of synchronization heretofore unachievable. The FCS family of systems is shown in Figure 3.



Figure 3. FCS- Family of Systems (Fonte : Army Transformation RoadMap)



Future Combat Systems will operate as a system of systems that will network existing forces, systems already under development, and complementary systems to be developed. The network will enable improved intelligence, surveillance and reconnaissance (ISR); enhanced analytical tools; joint exchange of blue and red force tracking down to the tactical level; battle command; real-time, sensor-shooter linkages; and increased synergy between echelons and within small units. It will also enable the UA to connect to units of employment, the next higher Army echelon; joint capabilities; and national assets. FCS will enable the networked maneuver unit of action to develop the situation in and out of contact, set conditions, maneuver to positions of advantage, and to close with and destroy the enemy.

The Future Combat Systems-equipped force represents a capability crucial to the Army's Future Force and the accomplishment of Department of Defense transformation goals. When fielded to the UA, FCS will provide the Future Force with unprecedented military capability for full-spectrum operations. Future Combat Systems are the key to achieving a strategically responsive, precision maneuver force that is dominant across the range of military operations as outlined for the Army's Future Force within the joint operations concepts (JOpsC).

### **FCS-Equipped Unit of Action (UA)**

The FCS-equipped UA is not just a unique brigade combat team built around a family of systems. Rather, it is the cornerstone of Future Force capabilities that demonstrates a new fighting concept. This formation provides the Joint Force with dominant land-power capability that is decisive in any operation, against any level threat, in any environment. The UA balances the capabilities for strategic responsiveness and battlespace dominance.

The UA can be tailored with additional capabilities for specific missions during a campaign. It allows command and control of up to six combined arms battalions by one commander. It is also able to employ a range of supporting capabilities to perform a variety of missions such as reinforcing fires, engineering operations, military police tasks, air and missile defense, psychological operations and civil affairs.

The UA is designed to ensure a campaign-quality Army. Although it has the responsiveness and deployability to achieve Army deployment goals, it is designed with the durability, endurance and stamina to fight battles and engagements for the duration of a campaign. Given its inherent tactical mobility, it can land at points removed from its objectives and out of range of enemy defenses, then move by land to complete its mission. This capability applies not only to entry operations, but also to theater operations throughout the campaign.

The FCS-equipped UA will be optimized to develop the situation out of contact, throwing the enemy off balance by destroying his high-payoff systems before forces are joined and maneuver to a position of advantage. The FCS-equipped UA sets the conditions and isolates enemy formations to enable it to close with and destroy the enemy at a time and place of its choosing.

Though the FCS-equipped UA will be optimized to develop the situation out of contact, it will be capable of finishing engagements decisively. FCS will be capable of providing the needed protection to ensure survivability. By the time FCS technologies mature, the Army expects to develop armor and other systems capable of defeating or mitigating emerging, improvised explosive device and man-portable anti-armor threats. Also, FCS will enable the Army to rapidly adapt and field improved survivability systems in response to emerging threats.

The FCS-equipped UA is a network-enabled force. Its vast sensor array will dramatically improve a commander's situational awareness. Sensor-shooter relationships begin with the Soldier and exist throughout the formation, allowing the UA to accurately direct internally generated effects or those generated from supporting units and joint assets. This ability to cooperatively engage targets with tactical, operational and strategic level assets will be accomplished in seconds rather than minutes. The UA presupposes platform superiority and emphasizes teaming of teams to achieve combat power synergy. FCS in its operational context is shown in Figure 4.

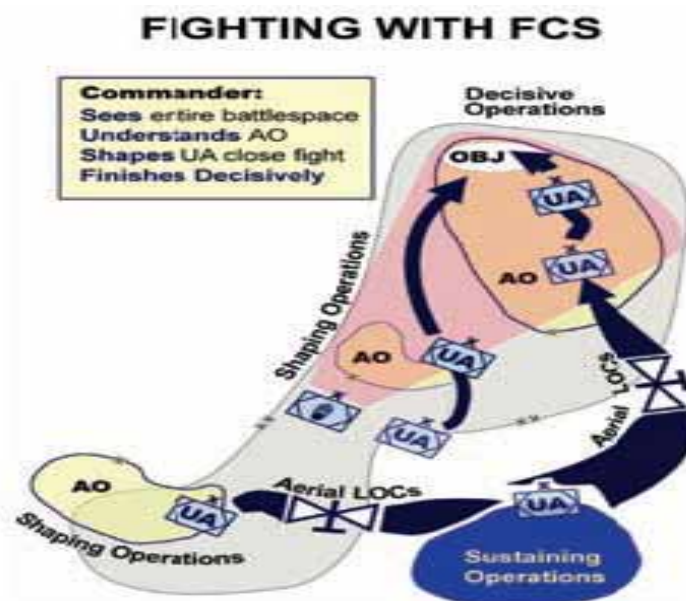


Figure 4. FCS-Equipped Unit's Operational Context (Fonte : Army Transformation RoadMap)

## Anexo E: Sistema de Informação e Comunicações Tático (SIC-T)<sup>53</sup>

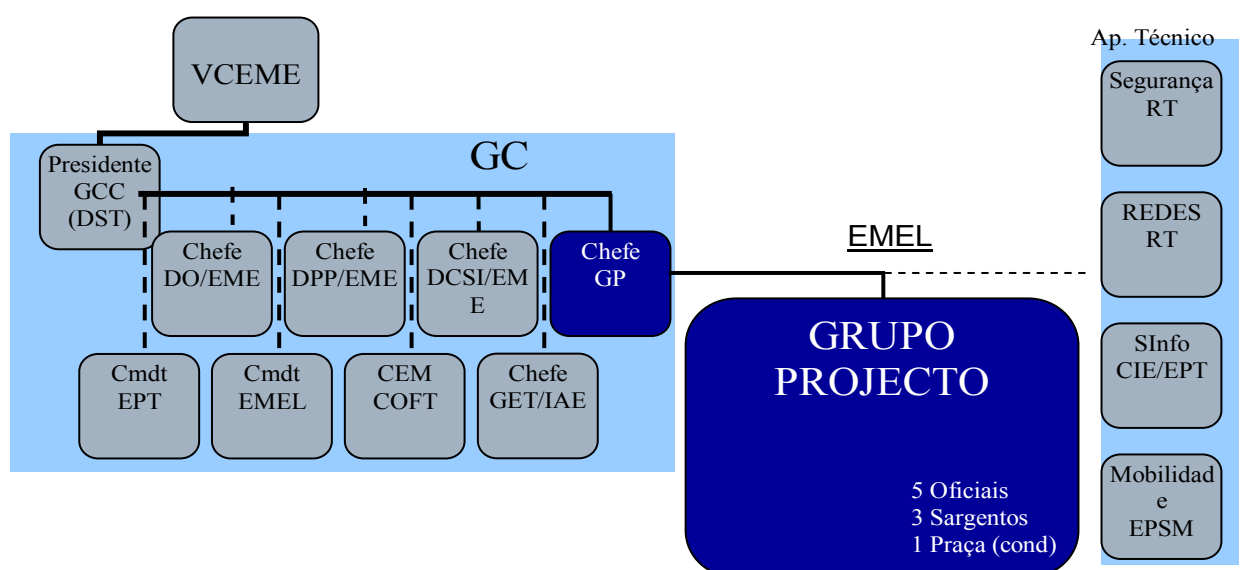
### SIC-T

O documento “Projecto SIC-T”, elaborado para dar cumprimento ao Despacho N.º 29/VCEME/2002, aprovado por Despacho do Exmo. TGEN VCEME de 27JAN04, define a arquitectura técnica e funcional para o futuro Sistema de Informação e Comunicações Tático do Exército, composto por uma componente de comunicações, o SITACO, e uma de informações, o SICCE.

O projecto **SIC-T** deverá, com base numa arquitectura técnica e funcional, possibilitar a implementação de unidades/órgãos ou módulos **SIC** destacáveis, típicos do escalão Brigada/Batalhão, com especial ênfase para a sua aplicabilidade em FNDs. Este projecto vai fornecer aos utilizadores os diferentes serviços totalmente integrados (*voz, mensagens, dados e imagem*), tendo em conta o equipamento existente bem como a perspectiva de implementação e ou aquisição de novos equipamentos, no âmbito da LPM.

O desenvolvimento e implementação deste Sistema de Informação e Comunicações, será efectuado em função dos requisitos operacionais da FOPE, tendo em consideração os cenários de emprego dentro do TN e em TO externos, a interligação com os Sistemas de Informação e Comunicações Estratégico e de Gestão (SIG), bem como a satisfação dos requisitos de interoperabilidade conjuntos e combinados, no âmbito da ONU, da OTAN, da UE e de coligações em que Portugal faça ou venha a fazer parte.

A estrutura de desenvolvimento e de coordenação do projecto é a indicada na figura seguinte:



<sup>53</sup>Info N.º12/2004 da DCSI/EME e PMLP

## SITACO

Os actuais sistemas de comunicações, baseados em *shelters*, garantem funcionalidades específicas, e possuem uma estrutura que se caracteriza por :

- grande rigidez, e deficiente flexibilidade e mobilidade;
- baixa capacidade de tráfego;
- comutação e gestão de rede efectuada de forma manual;
- ausência de sistemas de cifra *on line*,
- pouca fiabilidade devido à obsolescência da maioria dos equipamentos;
- necessidade de uma grande quantidade de homens e meios para operar;
- inexistência de interoperabilidade com outros sistemas, nacionais e aliados.

Para ultrapassar estas insuficiências, em 24 de Fevereiro de 97, com a aprovação dos “Requisitos Operacionais do **S**istema **T**ático de **C**omunicações do Exército - **SITACO**”, foram lançados os alicerces para o desenvolvimento e implementação de uma futura rede táctica de comunicações do Exército Português.

Este documento enquadrante define os requisitos operacionais e uma arquitectura geral de comunicações que permitirá o planeamento do futuro sistema táctico de comunicações.

A arquitectura da rede baseia-se em 4 subsistemas:

- O **Subsistema de Área Estendida (SAE)** constitui a espinha dorsal (*backbone*) da rede, sendo constituído por um conjunto de nós de comutação . A partir de cada um destes nós, que são designados nós de trânsito são sempre estabelecidos no mínimo dois *link's*, proporcionando caminhos alternativos e constituindo uma rede de estrutura malhada.
- O **Subsistema de Área Local (SAL)** fornece a um grupo de utilizadores localizado, normalmente num Posto de Comando (PC), as diversas categorias de teleserviços(Voz, Dados, Mensagens, fac-símile e vídeo) através de um nó de acesso. (Está previsto para este nós a comutação ATM em detrimento da tradicional comutação de circuitos; tem como vantagens, entre outras, a gestão dinâmica da largura de banda, e encaminhando a informação por circuitos com menor menor tráfego).
- O **Subsistema de utilizadores Móvel (SUM)** permite a ligação à rede táctica dos diversos utilizadores móveis. As categorias de Teleserviços previstos para este subsistema são os mesmos existentes no SAL, apenas com restrições na largura de banda utilizada. Os utilizadores deste subsistema podem aceder à rede num de três modos: rede rádio de combate (*Combat Net Radio - CNR*), rede rádio digital (pacotes)

(*Packet Radio Network - PRN*), ou acesso rádio através de canal selectivo (*Single Channel Radio Access - SCRA*). Cada utilizador móvel é automaticamente reconhecido por um Ponto de Acesso Rádio (*Radio Access Point - RAP*) que o interliga com a rede.

- **O Subsistema de Gestão e Controlo da Rede** (*System Management and Control Subsystem - SMCS*), que é responsável pelas funções de administração e controlo, constituindo-se como o “cérebro” da rede, permitindo que o Oficial de Comunicações possa supervisionar e controlar os equipamentos activos da rede.

